Maciej Laskowski

Współczesne Technologie Informatyczne

Techniki ochrony informacji

Partnerzy:

WSPÓŁCZESNE TECHNOLOGIE INFORMATYCZNE

TECHNIKI OCHRONY INFORMACJI

KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

Projekt Absolwent na miarę czasu współfinansowany przez Unię Europejską
w ramach Europejskiego Funduszu Społecznego

Wydział Elektrotechniki i Informatyki

Politechnika Lubelska
Wydział Elektrotechniki i Informatyki
ul. Nadbystrzycka 38A
20-618 Lublin

WSPÓŁCZESNE TECHNOLOGIE INFORMATYCZNE

TECHNIKI OCHRONY INFORMACJI

Maciej Laskowski

Politechnika Lubelska
Lublin 2013

Recenzenci:
dr hab. Stanisław Grzegórski, prof. Politechniki Lubelskiej
dr inż. Grzegorz Kozieł, Politechnika Lubelska

Projekt okładki: Maciej Laskowski

Skład komputerowy: Maciej Laskowski

Publikacja finansowana z projektu „Absolwent na miarę czasu"

Projekt „Absolwent na miarę czasu" współfinansowany przez Unię Europejską w ramach Europejskiego Funduszu Społecznego. Nr umowy UDA-POKL.04.01.01-00-421/10-01

Ta publikacja odzwierciedla jedynie stanowiska jej autorów, a Komisja Europejska nie ponosi odpowiedzialności za informacje w niej zawarte

Publikacja dystrybuowana bezpłatnie

Publikacja wydana za zgodą Rektora Politechniki Lubelskiej

ISBN: 978-83-63569-55-6

Wydawca: Politechnika Lubelska
ul. Nadbystrzycka 38D, 20-618 Lublin
Realizacja: Biblioteka Politechniki Lubelskiej
Ośrodek ds. Wydawnictw i Biblioteki Cyfrowej
ul. Nadbystrzycka 36A, 20-618 Lublin
tel. (81) 538-46-59, email: wydawca@pollub.pl
www.biblioteka.pollub.pl
Druk: TOP Agencja Reklamowa Agnieszka Łuczak
www.agencjatop.pl

Elektroniczna wersja książki dostępna w Bibliotece Cyfrowej PL www.bc.pollub.pl
Nakład: 100 egz.

SPIS TREŚCI

Wstęp 13

1 Wprowadzenie do problematyki ochrony informacji 14

1.1 Podstawowe pojęcia związane z ochroną informacji 15

1.2 Jednostki informacji 17

1.3 Szyfrowanie – podstawowe pojęcia i definicje 18

1.4 Elementy systemu teleinformatycznego istotne z punktu widzenia bezpieczeństwa 22

1.5 Ogólne problemy teorii ochrony informacji 22

2 „Klasyczne" techniki ochrony informacji 25

2.1 Początki technik ochrony informacji 26

2.2 Kryptografia symetryczna – techniki „klasyczne" 29

2.2.1 Metody podstawieniowe 32

2.3 Szyfry Agencji Wschodniej 58

2.4 ENIGMA 66

2.4.1 Powstanie enigmy 66

2.4.2 Budowa Enigmy 68

2.4.3 Enigma – sposób użycia 75

2.4.4 Złamanie szyfru Enigmy 77

2.5 Kryptografia symetryczna – techniki używane współcześnie 88
2.5.1 Szyfry blokowe 88
2.5.2 Szyfr książkowy 96
2.5.3 Szyfr z kluczem jednorazowym 98
3 Kryptografia asymetryczna i hybrydowa 101
3.1 Rys historyczny 102
3.2 Kryptografia asymetryczna – pojęcia i definicje 110
3.2.1 Funkcje jednokierunkowe 111
3.2.2 Klucz prywatny i publiczny 111
3.2.3 Protokół uzgadniania kluczy Diffiego – Hellmana 114
3.3 Wybrane algorytmy kryptografii asymetrycznej 115
3.3.1 RSA 115
3.3.2 ElGamal 116
3.3.3 Funkcje skrótu oraz DSA 117
3.4 Kryptografia hybrydowa 118
3.5 Techniki wykorzystujące kryptografię asymetryczną bądź hybrydową 118
3.5.1 TLS / SSL 118
3.5.2 SSH 122
3.5.3 IPSEC 123
3.5.4 Tunel 125
4 Polityka bezpieczeństwa systemów teleinformatycznych 127
4.1 Przegląd podstawowych zagrożeń i sposobów zabezpieczeń systemów teleinformatycznych 128
4.1.1 Zagrożenia fizyczne 129
4.1.2 Zagrożenia komunikacyjne (sieciowe) 130
4.1.3 Zagrożenia związane z oprogramowaniem 132

4.1.4 Zagrożenia związane z inżynierią społeczną 133
4.1.5 Pozostałe zagrożenia bezpieczeństwa 139
4.1.6 Zagrożenia dla systemów teleinformatycznych – podsumowanie 139
4.2 Strategia bezpieczeństwa 141
4.2.1 Określenie zasobów systemu 142
4.2.2 Oszacowanie ryzyka 142
4.2.3 Zagadnienia związane z ryzykiem 146
4.2.4 Regulacje prawne dotyczące bezpieczeństwa teleinformatycznego 146
4.2.5 Analiza kosztów i zysków 148
4.3 Polityka bezpieczeństwa systemów teleinformatycznych 148
4.3.1 Różnice pomiędzy polityką a strategią bezpieczeństwa 149
4.3.2 Wymagania stawiane polityce bezpieczeństwa 150
4.3.3 Elementy polityki bezpieczeństwa 151
4.3.4 Implementacja polityki bezpieczeństwa 155
4.4 Model bezpieczeństwa 156
4.4.1 Wady i zalety omówionych modeli bezpieczeństwa 157
5 Kierunki rozwoju technik ochrony informacji 159
5.1 Kryptografia kwantowa 160
5.1.1 Szyfrowanie kwantowe 160
5.1.2 Wymiana kluczy w kryptografii kwantowej 161
5.1.3 Kryptoanaliza kwantowa 163
5.2 Wieloplatformowe techniki ochrony informacji 163
Posłowie 165
Bibliografia 166

Dla J. i S.

- za wszystko

M

WSTĘP

Od zarania dziejów człowiek dążył do zachowania pewnych tajemnic tylko dla siebie lub dla wąskiej grupy zainteresowanych. Działo się tak z wielu powodów – dochowanie sekretu oznaczało bogactwa płynące z handlu, umożliwiało prowadzenie zwycięskich wojen, potajemne spotkania czy też po prostu gwarantowało osobiste bezpieczeństwo.

W przeciągu ostatnich dwustu lat techniki ochrony informacji uległy praktycznie całkowitej zmianie – proste podstawianie liter lub znaków zostało szybko wyparte przez znacznie bardziej zaawansowane metody ukrywania tekstu jawnego, jak chociażby metoda macierzowa czy *le chiffre indechiffrable*...

Co więcej, od początku XX wieku zadania szyfrantów coraz częściej zaczęły przejmować maszyny. Oznaczało to prawdziwy rozwój kryptografii – wystarczy wspomnieć takie hasła jak Enigma, japońskie maszyny szyfrujące czy pierwsze superkomputery...

Dopiero od niedawna żyjemy w epoce prawdziwej rewolucji w technikach ochrony informacji – stało się to za sprawą genialności kluczy asymetrycznych i rozwoju idei kryptografii kwantowej.

Do połowy XX wieku rozwiązania kryptologiczne stosowało głównie wojsko oraz instytucje rządowe. Dopiero w przeciągu ostatniego półwiecza, wraz z postępem w elektronice, informatyce oraz telekomunikacji, rozwinęła się również kryptologia

cywilna, która znalazła szerokie spektrum zastosowań – począwszy od wymiany informacji finansowej i biznesowej, na komunikacji międzyludzkiej (poczta elektroniczna, komunikatory) skończywszy.

Dzięki szybkiemu rozwojowi Internetu oraz związanych z nim technologii informacja nabrała realnej wartości. Każdego dnia przez światową sieć przesyłane są olbrzymie ilości danych. Duża część z nich ma charakter typu *public access*, co oznacza, że są dostępne dla każdego, kto chce się z nimi zapoznać. Internet jednak jest używany również do wymiany danych uznawanych za *prywatne*, *poufne*, czy nawet *tajne*. Są one często podstawą działania wielu firm i organizacji – w tym przypadku za priorytetowe należy uznać zapewnienie integralności oraz odpowiednich praw dostępu. Spełnienie tych wymagań jest niezbędne do utrzymania przewagi nad konkurencją, zarówno w świecie biznesu, jak i organizacji naukowo-badawczych.

W niniejszej książce postaramy się prześledzić drogę, jaką pokonały w ciągu tysiącleci techniki ochrony informacji, stając się z instrumentu władzy elementem codziennego życia w epoce cyfrowej. Przyjrzymy się, jakich szyfrów używał Cezar oraz średniowieczni alchemicy, myśliciele czasu Odrodzenia i dziewiętnastowieczni spiskowcy, geniusze, dwudziestowieczni wojskowi stratedzy i zwykli ludzie.

Na łamach tej książki postaramy się poznać sylwetki ludzi, którzy zadali sobie kilka ważnych pytań:

Dlaczego nie można wykorzystywać kryptografii do ochrony prywatności zwykłych obywateli?

Dlaczego nie można stworzyć systemu gwarantującego stuprocentowe zachowanie tajemnicy?

Kto i dlaczego hamuje rozwój światowej, powszechnie dostępnej kryptografii?

Poznamy również ludzi, którzy za wszelką cenę starali się uniknąć na nie odpowiedzi.

Ci pierwsi byli społecznymi outsiderami – akademickimi wolnomyślicielami, idealistami swojej epoki, czy też, jak sami się później ochrzcili, *szyfropunkami*, mającymi do dyspozycji tylko zapał, wolny umysł oraz swoje własne ideały.

Ci drudzy zaś byli wówczas najpotężniejszymi osobami na świecie – wojskowymi, politykami, przywódcami państw, dysponującymi najnowocześniejszą technologią, wielomiliardowym budżetem oraz potężnym zapleczem polityczno-gospodarczym.

Postaramy się wspólnie odsłonić kulisy kryptograficznej wojny, która toczyła się przez ostatnie stulecia, i która jeszcze się nie skończyła.

Ale spróbujcie zgadnąć, kto póki co wygrywa...

Autor

1

Wprowadzenie do problematyki ochrony informacji

Cel

Wprowadzenie do problematyki ochrony informacji. Omówienie podstawowych pojęć oraz terminów wykorzystywanych w dalszej części książki. Wprowadzenie do problematyki szyfrowania. Omówienie i analiza ogólnych problemów związanych z technikami ochrony informacji.

Plan

1. Podstawowe pojęcia związane z ochroną informacji
2. Jednostki informacji
3. Szyfrowanie – podstawowe pojęcia i definicje
4. Ogólne problemy technik ochrony informacji

1.1 PODSTAWOWE POJĘCIA ZWIĄZANE Z OCHRONĄ INFORMACJI

Przedstawienie problematyki ochrony danych należy rozpocząć od zdefiniowania kilku podstawowych pojęć.

Dane (ang. *data*, z łac. *datum* – to, co jest dane) – w fizyce i matematyce to wartości znane w rozwiązywaniu problemów fizycznych czy matematycznych, np. zadań (Słownik języka polskiego PWN, 2012). W języku potocznym, dane to otrzymane informacje lub wiadomości używane do wyciągania jakichś wniosków. W najbardziej ogólnym systemowym sensie dane są zdefiniowane jako wszystko, co jest/może być przetwarzane umysłowo lub komputerowo (Gadomski, 2003).
W tym sensie dane są pojęciem relatywnym, istnieją tylko razem z pojęciem przetwarzania i mogą przyjmować takie postaci jak: znaki, mowa, wykresy i sygnały (Gadomski, 2003).

Informacja (łac. *informatio* – przedstawienie, wizerunek) to termin interdyscyplinarny, którego definicje różnią się, w zależności od dziedziny nauki. Najogólniejsza definicja informacji to: jest to właściwość pewnych obiektów (Cackowski, Kmita & Szaniawski, 1987) lub relacja między elementami zbiorów pewnych obiektów, której istotą jest zmniejszanie niepewności, nieokreśloności (Wielka Encyklopedia PWN, 2002).

Oznacza to, że różne dane mogą dostarczać tą samą informację, ale jednocześnie te same dane mogą też dostarczać różnych informacji. Z drugiej strony, np. zbiory liczb czy wyrazów mogą być danymi, ale jeśli nie wiemy, co reprezentują, to nie są one informacją.

Kolejnym istotnym pojęciem, które wymaga przyjęcia w miarę jednoznacznej definicji jest **bezpieczeństwo**, które w informatyce to występuje w dwóch znaczeniach: *security* – czyli ochrony danych w sieciach i systemach komputerowych oraz *safety* – odporności tychże sieci i systemów na awarie, zarówno te wynikające z ich nieuniknionej zawodności, jak i z wpływu czynników zewnętrznych bez względu

na ich źródło (Laskowski, 2007). Tak więc system komputerowy może zostać uznany za bezpieczny, jeśli jego użytkownik może oczekiwać, że informacja, którą do niego wprowadzi na stałe nie zostanie utracona, zmodyfikowana ani użyta w sposób nieautoryzowany lub przypadkowy.

Kolejnym istotnym pojęciem jest **kryptologia**, czyli nauka o przekazywaniu informacji w sposób zabezpieczony przed niepowołanym dostępem – czy to w celu modyfikacji, czy też zapoznania się z ich treścią (Schneier, 2002).
Kryptologia dzieli się na (za: Schneier, 2002):

- kryptografię – czyli naukę o tworzeniu systemów kryptograficznych;
- kryptoanalizę – czyli naukę o ich łamaniu.

Kryptologia obejmuje między innymi trzy podstawowe zagadnienia z dziedziny bezpieczeństwa danych, które zostały określone za pomocą angielskiego akronimu **CIA** (za: Schneier, 2002, Starościak, 2004):

- *poufność* (ang. *Confidelity*) – informacja nie może zostać odczytana bez znajomości klucza użytego do jej zaszyfrowania;
- *nienaruszalność* (ang. *Integrity*) – zarówno nadawca, jak i odbiorca mają pewność, że informacja nie została zmieniona;
- *kontrola dostępu* (ang. *Access control*) – treść nadawanej informacji są w stanie odczytać jedynie upoważnione osoby (posiadające klucz szyfrujący).

Dodatkowo, kryptologia obejmuje również (za: Schneier, 2002; Starościak, 2004):

- *uwierzytelnianie* (autentykacja) – nadawca może udowodnić odbiorcy swoją tożsamość;
- *niezaprzeczalność* – odbiorca może udowodnić tożsamość nadawcy.

Bezpieczeństwo jest elementem szerszego kontekstu, określanego jako **wiarygodność systemu informatycznego** (Schneier, 2002). Jest to atrybut tzw. wysokiego poziomu, co oznacza, że można go podzielić na bardziej szczegółowe pod-atrybuty (za: Sacha, Cegieła & Zalewski, 2012; Szychowiak, 2012):

- *niezawodność* – czyli zdolność systemu do nieprzerwanego dostarczania usług oczekiwanych przez użytkowników w określonych warunkach funkcjonowania;
- *dyspozycyjność*, niekiedy łączona także z pojęciem niezawodności (np. Szychowiak, 2012) – czynnik określający procent czasu, w którym system może świadczyć oczekiwane usługi we wspomnianych warunkach funkcjonowania;
- *bezpieczeństwo* (ang. *safety*) – system musi gwarantować bezpieczeństwo otoczenia (środowiska pracy) w przypadku awarii;
- *bezpieczeństwo* (ang. *security*) – system musi zapewniać ochronę danych wprowadzonych do niego przez upoważnionych użytkowników;
- *autentyczność* – musi istnieć skuteczna metoda weryfikacji tożsamości użytkowników.

Jak można więc zauważyć, kryptologia oraz bezpieczeństwo mają wiele wspólnych elementów – i często trudno jest jednoznacznie stwierdzić, które zagadnienie powinno być rozpatrywane w kontekście kryptologicznym, które zaś w kontekście bezpieczeństwa.

1.2 JEDNOSTKI INFORMACJI

Bit (ang. kawałek, skrót od *binary digit*, czyli dosłownie: cyfra dwójkowa) to najmniejsza ilość informacji potrzebna do określenia, który z dwóch równie prawdopodobnych stanów przyjął układ (Baczyński, Janoś & Kaczmarek, 2000).
Jest to również najmniejsza jednostka informacji używana w odniesieniu do sprzętu komputerowego. Oznaczana jest jako „b”.

Binarny sposób zapisu informacji związany jest z tym, że komputer jako urządzenie cyfrowe rozpoznać może dwa stany napięciowe:

- 0 – brak napięcia lub bardzo niskie (mniej niż 10% wartości wysokiego);
- 1 – wysokie napięcie.

Bit przyjmuje jedną z dwóch wartości, które zwykle określa się jako 0 (zero) i 1 (jeden), choć można przyjąć dowolną inną parę wartości, np. *prawda* i *fałsz*, *tak* lub *nie* czy też -1 i +1 (Baczyński, Janoś & Kaczmarek, 2000).

Nat jest jednostką ilości informacji mierzonej przez logarytm naturalny ilości możliwości.

$$1 \text{ nat} = \log_2(e) \text{ bitów}$$

$$1 \text{ bit} = \ln(2) \text{ natów}$$

Hartley (określany także jako **ban** lub też jako **dit** od *decimal digit*) to jednostka informacji lub entropii. Jeden hartley to ilość informacji zawarta w wiadomości o zajściu zdarzenia, którego prawdopodobieństwo wynosi 0,1 (Abramson, 1963).

Konstrukcja tej miary informacji oparta jest o logarytm o podstawie 10 (dziesiętny), podczas gdy bit jest jednostką miary informacji opartą o logarytm o podstawie 2 (dwójkowy). Podobnie jak bit odpowiada cyfrze dwójkowej, ban odpowiada cyfrze dziesiętnej.

Jeden ban to około 3,32 bitu – $\log_2(10)$ lub 2,30 nata – $\ln(10)$ (Abramson, 1963).

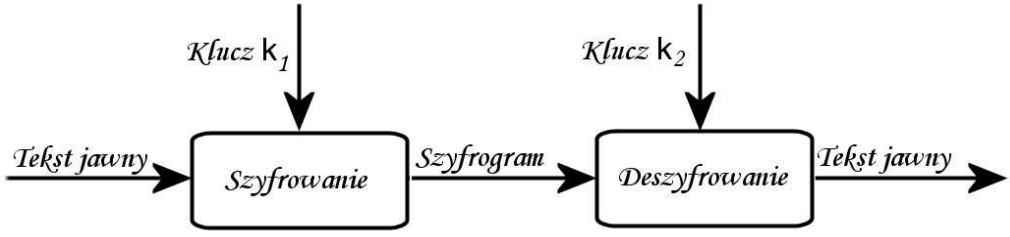
Należy zauważyć, że spośród wymienionych powyżej jednostek to właśnie bit znajduje najszersze zastosowanie w informatyce.

1.3 SZYFROWANIE – PODSTAWOWE POJĘCIA I DEFINICJE

Utajnienie oraz kontrola dostępu realizowane są poprzez **zaszyfrowanie** wiadomości, czyli poprzez procedurę przekształcenia zawartych w niej informacji w taki sposób, aby były one czytelne jedynie dla uprawnionych osób (Garbarczuk & Świć, 2005).

Wiadomość przed zaszyfrowaniem określa się mianem **tekstu jawnego** (ang. *plaintext*), zaś wiadomość zaszyfrowaną – **szyfrogramu** (ang. *ciphertext*) (Garbarczuk & Świć, 2005).

Ogólny schemat procesu szyfrowania został przedstawiony na rysunku 1.1.



Rys. 1.1. Ogólny schemat procesu szyfrowania (źródło: Garbarczuk & Świć, 2005)

Idea szyfrowania opiera się na dwóch elementach: algorytmie szyfrującym i kluczu.

W literaturze (np. (Pieprzyk, Hardjono & Seberry, 2006; Garbarczuk & Świć, 2005) wymieniane są następujące cechy, jakie powinien spełniać mocny algorytm kryptograficzny:

- złożoność matematyczna algorytmu szyfrującego powinna wykluczać możliwość stosowania metod analitycznych do złamania szyfru;
- koszt lub czas wymagany dla uzyskania klucza lub odczytania tekstu jawnego z kryptogramu powinien być znaczny i praktycznie nie do przyjęcia.

Algorytm szyfrujący powinien spełniać powyższe warunki nawet wówczas, gdy kryptoanalityk posiada dostęp do względnie dużej porcji tekstów jawnych i odpowiadających im kryptogramów, a także, gdy zna on dokładnie wszelkie detale algorytmu. Bezpieczeństwo szyfru nie może więc polegać na tajności algorytmu szyfrującego, ale na tajności klucza wykorzystanego do szyfrowania (Schneier, 2002).

Pojęciem **klucza** (ang. *key*) określa się w kryptografii informację umożliwiającą wykonanie pewnej czynności kryptograficznej – szyfrowanie, deszyfrowanie, podpisywanie informacji, weryfikacja podpisu, etc. (Schneier, 2002). Im większa jest długość klucza, tym więcej możliwych kombinacji. Długość 32 bitów oznacza, iż klucz może przyjąć jedną z 2^{32} wartości. Zwiększenie długości klucza o jeden bit (np. do 33 bitów) powoduje podwojenie liczby możliwych wartości klucza (do 2^{33}).

Ze względu na rodzaj zastosowanego klucza wyróżniamy podział na (za: Schneier, 2002):

- kryptografię symetryczną, w której ten sam klucz używany jest zarówno do szyfrowania, jak i deszyfrowania informacji i z tego powodu powinien być znany tylko upoważnionym uczestnikom transmisji;
- kryptografię asymetryczną, w której używa się zestawów dwu (najczęściej) lub więcej powiązanych ze sobą kluczy, umożliwiających wykonywanie różnych czynności kryptograficznych.

Kryptografia symetryczna udostępnia jedynie szyfrowanie – wszystkie bardziej zaawansowane funkcje kryptograficzne, takie jak podpisy cyfrowe, uwierzytelnianie, etc. dostępne są tylko w kryptografii asymetrycznej (Garbarczuk & Świć, 2005).

Przedstawione powyżej rodzaje kryptografii zostaną dokładniej omówione (wraz z historycznymi przykładami) w następnych rozdziałach.

Obecnie w praktyce stosuje się algorytmy, których źródła są powszechnie znane i które przez wiele lat stosowania oparły się kryptoanalizie – dzięki temu mogą zostać uznane za wiarygodne (Garbarczuk & Świć, 2005). Algorytmy, których trudność deszyfrowania szyfrogramu opiera się o ukrycie źródeł algorytmu określa się mianem **algorytmów ograniczonych**, są one jednak uważane za niewiarygodne (Garbarczuk & Świć, 2005).

Proces szyfrowania i deszyfrowania można opisać następująco:

$$E_{ks}(P)=C$$

$$D_{kd}(C)=P$$

gdzie:

P – tekst jawny wiadomości,

C – szyfrogram,

E – funkcja szyfrująca,

D – funkcja deszyfrująca,

ks – klucz szyfrujący,

kd – klucz deszyfrujący.

Powyższe wzory można zapisać również w postaci:

$$D_{kd}(E_{ks}(P)=P$$

Istotą **steganografii** jest przekazywanie tajnych informacji w taki sposób, aby nie ujawniać osobom postronnym ich istnienia ani samego faktu ukrytej komunikacji.

Steganografia jest odmienna od kryptografii, której celem jest ochrona treści przesyłanej wiadomości przed jej odczytaniem przez osoby nieuprawnione, przy czym sam fakt komunikacji może być znany (Lubacz, Mazurczyk & Szczypiorski, 2010).
Do przeprowadzenia steganograficznej wymiany danych jest niezbędne wykorzystanie nośnika, w którym ukryte zostaną informacje.
Aby nadawał się on do prowadzenia ukrytej komunikacji, muszą zostać spełnione dwa podstawowe warunki (za: Lubacz, Mazurczyk & Szczypiorski, 2010):

- wprowadzenie ukrytej wiadomości nie może powodować łatwo wykrywalnych zmian samego nośnika;
- nośnik powinien być powszechnie wykorzystywany.

Pod pojęciem **poziomu bezpieczeństwa** określa się w kryptografii liczbę bitów oznaczającą ile razy maksymalna liczba obliczeń, które musi wykonać atakujący (podsłuchujący transmisję teleinformatyczną), jest większa od liczby obliczeń, które musi wykonać uprawniony uczestnik tej transmisji (Garbarczuk & Świć, 2005).

Poziom bezpieczeństwa *k* oznacza, że atakujący musi wykonać *2k* razy więcej operacji od uprawnionego uczestnika. Oczywiście jest to założenie teoretyczne – w praktyce istnieje prawdopodobieństwo, iż podsłuchujący transmisję może odkryć właściwy klucz np. po przejrzeniu połowy przestrzeni poszukiwań (co powinno obniżyć poziom bezpieczeństwa o 1 bit). Co więcej, poziom ten może ulec zmniejszeniu w miarę postępów w kryptoanalizie.

Poziom bezpieczeństwa wyrażony jest w bitach, gdyż liczba ta często odpowiada długości klucza lub długości wyniku funkcji skrótu (w bitach). Należy jednak podkreślić, że poziom bezpieczeństwa nie jest równoważny długości klucza (Garbarczuk & Świć, 2005).

1.4 ELEMENTY SYSTEMU TELEINFORMATYCZNEGO ISTOTNE Z PUNKTU WIDZENIA BEZPIECZEŃSTWA

Analizując temat bezpiecznego systemu teleinformatycznego należy dokonać jego podziału na pięć podstawowych kategorii:

- algorytmy kryptograficzne;
- sprzęt komputerowy;
- oprogramowanie i dane użytkownika;
- infrastruktura sieciowa;
- zabezpieczenia fizyczne.

Prawidłowo zaprojektowany system informatyczny powinien pokrywać elementy należące do każdej z wymienionych powyżej kategorii. Nie można bowiem stworzyć systemu informatycznego spełniającego zdefiniowane powyżej wymagania dotyczące bezpieczeństwa bez zapewnienia odpowiednich zabezpieczeń na każdej jego płaszczyźnie – zarówno logicznej, jak i sprzętowej (fizycznej).

1.5 OGÓLNE PROBLEMY TEORII OCHRONY INFORMACJI

Problematyka tworzenia zabezpieczeń podlega pewnym ogólnym prawom, wynikającym zarówno z logiki, ekonomii jak i ograniczeń technologicznych. Pozwala to na sformułowanie kilku truizmów obowiązujących podczas tworzenia i wdrażania ochrony systemu informatycznego, które będą stanowiły podstawę do dalszych rozważań dotyczących technik ochrony informacji.

Są to m.in.:

- Nie istnieje stuprocentowo bezpieczny system informatyczny.

  Eugene Spafford, jeden z najbardziej znanych specjalistów od technologii zabezpieczeń komputerowych sformułował to twierdzenie w następującej postaci:

  Prawdziwie bezpieczny system to taki, który został odłączony od prądu, umieszczony w wyłożonym ołowiem betonowym pomieszczeniu, które zostało

otoczone strażnikami... Ale nawet wtedy miałbym wątpliwości… (Garfinkel & Spafford, 1991).

To ironiczne zdanie najlepiej chyba ilustruje fakt, że twórcy systemów teleinformatycznych nigdy nie będą w stanie przewidzieć wszystkich możliwych zagrożeń, zwłaszcza, że ich największym wrogiem jest rozwój technologii.

- *Szybkość jest duszą wojny, wykorzystaj swoje szanse zanim przeciwnik osiągnie gotowość* (Sun Tzu, 2008).

  Czas reakcji na zmiany – na przykład na nowo odkryte luki w stosowanym oprogramowaniu bądź technikach ochrony danych – nigdy nie będzie zerowy. Dlatego nawet w przypadku dopracowanego i dobrze administrowanego systemu zabezpieczeń istnieje ryzyko, że przez pewien okres stosowane mechanizmy ochrony będą nieskuteczne.
- Kolejnym czynnikiem, który ma znaczący wpływ na spadek poziomu bezpieczeństwa jest człowiek. Lukę w zabezpieczeniach może stanowić zarówno błąd programisty czy projektanta systemu, jak i niefrasobliwość czy też nieostrożność użytkowników.

  Powstaje więc pytanie – *w którym momencie można uznać system teleinformatyczny za wystarczająco bezpieczny, skoro nie jest możliwe zapewnienie całkowitej jego ochrony*?

  Aby uzyskać najbardziej logiczną odpowiedź należy postawić się w miejscu potencjalnego atakującego. Im więcej zabezpieczeń agresor będzie musiał pokonać, im bardziej atak będzie nieopłacalny (czy to pod względem mocy obliczeniowej czy też np. czasochłonności), tym mniej chętnie będzie podejmował próby. Szczególne znaczenie ma tutaj czynnik czasu – informacja (przynajmniej w większości przypadków) posiada wartość tak długo, jak jest aktualna.
- Każdy łańcuch jest tak mocny, jak jego najsłabsze ogniwo. Można tutaj odwołać się do znanej analogii z pancernymi drzwiami – po co włamywacz miałby je wyważać, jeśli może wejść przez rozbite okno? Projektanci zabezpieczeń muszą pamiętać, że atakujący na ogół nie będzie się skupiał na pokonywaniu przeszkód, tylko będzie się starał je obejść.

Zazwyczaj jest to rozwiązanie mniej czasochłonne, a co za tym idzie mniej kosztowne i mniej ryzykowne niż łamanie zabezpieczeń.

Prawdziwa umiejętność to złamanie oporu przeciwnika bez walki (Sun Tzu, 2008).

- Jedna linia obrony to stanowczo za mało. Obejście jednego mechanizmu zabezpieczeń często okazuje się być możliwe – tak więc naturalną konsekwencją dla projektanta powinno być opracowanie wielu zróżnicowanych linii ochrony, tak, aby pokonanie jednej z nich nie doprowadziło do przejęcia kontroli nad całym systemem.

  Dodatkowo dywersyfikacja mechanizmów obronnych stanowi dodatkową ochronę w przypadku awarii określonego typu elementów zabezpieczających – żadna usterka nie może powodować otwarcia niekontrolowanego kanału dostępowego do chronionego systemu teleinformatycznego.
- Wąskie przejście ogranicza również możliwości ataku. Im mniej kanałów łączy system informatyczny ze światem zewnętrznym, tym łatwiej jest je kontrolować i chronić.
- Złudne poczucie bezpieczeństwa jest gorsze od jego braku. Wielu administratorów popełnia błąd sądząc, że dopóki nie ma odnotowywanych symptomów naruszenia bezpieczeństwa systemu, oznacza to, że wszystko jest w porządku. Wiele ataków czy incydentów wykrywanych jest *post factum*, nawet w przypadku stale i poprawnie monitorowanych systemów teleinformatycznych. Ważne jest więc, aby ciągle testować i udoskonalać mechanizmy zabezpieczeń.

  Trzeba podważać wszystko, co się da podważyć, gdyż tylko w ten sposób można wykryć to, czego podważyć się nie da (Gagavai, 2012).

2

„Klasyczne” techniki ochrony informacji

Cel

Omówienie historycznych technik ochrony informacji. Omówienie podstawowych pojęć oraz terminów wykorzystywanych w dalszej części rozdziału. Kryptografia symetryczna. Omówienie i analiza maszyn szyfrujących na podstawie Enigmy.

Plan

1. Historyczne techniki ochrony informacji
2. Kryptografia symetryczna – podstawowe pojęcia i definicje
3. Algorytmy i metody szyfrowania symetrycznego
4. Maszyny szyfrujące – *casus* Enigmy

2.1 POCZĄTKI TECHNIK OCHRONY INFORMACJI

Historycznie najstarszą metodą ochrony informacji była steganografia, umożliwiająca przekazanie informacji pomiędzy zainteresowanymi stronami w taki sposób, aby obecność komunikatu nie została wykryta. Dodatkowo, w odróżnieniu od kryptografii, gdzie obecność komunikatu nie jest negowana natomiast jego treść jest niejawna, steganografia próbuje ukryć także fakt prowadzenia komunikacji pomiędzy stronami.

Jej efektywność zależy jednak od wyrafinowania zatajającego i zdolności strony przechwytującej, uporu w szukaniu bądź analizy środka przekazu.

Pierwsze wzmianki o użyciu technik steganograficznych do ochrony informacji można odnaleźć w *Dziejach* Herodota z V wieku p.n.e., czyli kronice konfliktów persko-greckich.

Grecki uchodźca Demaratos obserwował przygotowania Persów do ataku. Chcąc ostrzec Spartan o planach perskiego władcy Kserksesa musiał wymyśleć taki sposób przesłania listu, aby nie przechwycili go perscy strażnicy.

Nie mogąc zaś w inny sposób tego uczynić, z obawy, aby go nie przyłapano, wymyślił co następuje. Wziął podwójną tabliczkę, zeskrobał z niej wosk, a następnie na drzewie tabliczki wypisał zamiar króla; uczyniwszy to, polał znowu litery woskiem, aby niosącemu próżną tabliczkę nie przyczyniła jakiego kłopotu ze strony straży strzegącej drogi. Kiedy tabliczka istotnie dotarła do Lacedemonu, nie mogli Lacedemończycy zgadnąć, co ona oznacza, aż (jak słyszę), córka Kleomenesa, a żona Leonidasa, Gorgo, jedyna ich pouczyła. Ona to po namyśle kazała im zeskrobać wosk, mówiąc, że odnajdą litery na drzewie. Usłuchali, znaleźli i odczytali, a następnie dali znać reszcie Hellenów. To więc tak podobno się stało (Herodot, 1959).

Po otrzymaniu tego ostrzeżenia Grecy zaczęli się zbroić, zaś sam konflikt grecko-perski jest z pewnością znany czytelnikowi chociażby z bitwy pod Termopilami.

Herodot w *Dziejach* opisał też inny sposób tajnego przekazu informacji: były tyran Histiajos, przetrzymywany przez króla perskiego Dariusza, postanowił przesłać

informację do swego zięcia Arystagorasa z Miletu, aby ten przyczynił się do wybuchu powstania miast jońskich. Jednak wiadomość należało przesłać tak, aby mogła się ona przedostać mimo pilnujących go strażników. By tego dokonać Histiajos wytatuował ją na wygolonej głowie swego niewolnika. Kiedy niewolnikowi odrosły włosy posłał go z oficjalnym, mało istotnym listem. Posłaniec, który nie miał przy sobie nic, co mogło by budzić wątpliwości straży bez przeszkód udał się do Miletu, ponownie ogolił głowę i skłonił ją przed Arytogorasem. Reagując na wybuch powstania, Dariusz wysłał Histiajosa do Jonii w roli mediatora. Grek miał jednak własne plany polityczne i przyłączył się do antyperskiego powstania. Histajosowi nie udało się jednak zjednoczyć Hellenów i objąć nad nimi przywództwa. Były tyran Miletu błąkał się na czele nielicznej floty między wyspami, łupiąc kolejne miasta i zatapiając liczne statki handlowe wroga, by ostatecznie dostać się do perskiej niewoli i zostać w niej straconym (Hammond, 1973).

W ciągu następnych wieków od czasów Herodota na całym świecie zaczęto stosować różne metody steganografii. Pliniusz Starszy już w I wieku n.e. twierdził, że sok rośliny *tithymallus* można wykorzystać jako atrament do pisania tajnych wiadomości – po wyschnięciu napis staje się niewidoczny, ale zwęgla się pod wpływem ciepła, co umożliwia odczytanie komunikatu (Singh, 2003).

Starożytni Chińczycy pisali listy na cienkim jedwabiu, który następnie ugniatano w kulkę, którą przed połknięciem przez posłańca pokrywano woskiem.

Szesnastowieczny włoski uczony Giovanni Della Porta opisywał sposób ukrywania wiadomości w ugotowanym na twardo jajku – na skorupce jajka umieszczano komunikat, zapisując go przy użyciu specjalnego atramentu, który przenikał przez porowatą skorupkę, dzięki czemu dostęp do informacji można było uzyskać dopiero po jej rozbiciu (Kahn, 1997).

Choć steganografia może być w wielu przypadkach wystarczającą metodą do zatajenia informacji, to jej efektywność zależy wyłącznie od tego czy zostanie odkryta, czy nie: przechwycenie wiadomości oznacza ujawnienie tajemnicy. Przykładowo, gdyby straże perskie zdjęły wosk z tablic, które wydawały się puste, wojna potoczyłaby się zupełnie inaczej. Ukrycie wiadomości na głowie posłańca trwało dosyć długo (przynajmniej kilka tygodni). Ogrzanie pozornie pustych (lub nawet zapisanych) kartek papieru również nie stanowi dużej trudności.

Z powodu tej oczywistej słabości tak prostych technik steganograficznych, wynalezienie kryptografii stało się koniecznością.

Jak zostało wspomniane w poprzednim rozdziale, celem kryptografii nie jest ukrycie istnienia wiadomości (czy też faktu komunikacji pomiędzy dwiema stronami), lecz utajnienie jej znaczenia.

Stanowi to o przewadze kryptografii nad steganografią, gdyż nawet, jeśli komunikat zostanie przechwycony przez osobę nieupoważnioną, to nie może ona jej odczytać (w prosty sposób) bez znajomości procedury szyfrującej (i klucza).

Wprawdzie kryptografia i steganografia są od siebie niezależne, nie zmienia to jednak faktu, że często metody te łączy się w celu zwiększenia poziomu bezpieczeństwa przesyłanej wiadomości.

Przykładem może być tutaj metoda mikropunktu, która sama zalicza się do technik steganograficznych: właściwa wiadomość jest zmniejszana przy użyciu technik fotograficznych do niewielkich rozmiarów, zaś następnie dołączana jest do wiadomości mało istotnej, jako jej fizyczny fragment. Współczesne mikropunkty wykorzystują skalę miniaturyzacji około 300:1, co oznacza możliwość pomniejszenia kartki formatu A4 do wielkości pojedynczej kropki znajdującej się w tekście pisanego czcionką normalnej (10-12 punktów) wielkości listu (Piekałkiewicz, 1999).

Pierwsze próby miniaturyzowania przesyłanych informacji za pomocą mikrofotografii podjęto w 1870 podczas wojny francusko-pruskiej.

Raporty do oblężonego przez Niemców Paryża przesyłane były w postaci prostokątów o wymiarach 3cm na 4cm – wynikało to jednak nie z chęci zachowania niejawności, a z ograniczeń nośnika, jakim były gołębie pocztowe (Kipper, 2003).

Technika mikropunktu została udoskonalona w trakcie II wojny światowej przez Abwehrę: uzyskano mikropunkt wielkością porównywalny do kropki uzyskiwanej na ówcześnie używanej zwykłej maszynie do pisania (White, 1992). Sposób ten oferował nowe możliwości w przesyłaniu dużych ilości informacji w sposób trudny do wykrycia – mikropunkt można było umieścić pod znaczkiem pocztowym, banderolą paczki papierosów lub w rozciętym żyletką rogu kartki pocztowej lub w dowolnie innym wybranym miejscu np. w tekście korespondencji jako kropka kończąca zdanie (Piekałkiewicz, 1999). Warto również zauważyć, że metoda ta pozostała niewykryta aż do chwili, w której FBI otrzymało wskazówkę,

aby poszukiwać niewielkich odbłysków na powierzchni listu, które były spowodowane odbiciem światła od kliszy filmu (Singh, 2003). Spowodowało to konieczność połączenia przez Niemców technik steganograficznych z kryptograficznymi: wiadomość przez zmniejszeniem szyfrowano, dzięki czemu nawet jeśli agentom FBI udało się przechwycić lub zablokować wymianę informacji, nie mogli oni się niczego dowiedzieć o działalności niemieckich agentów (Singh, 2003).

Warto zauważyć, że współcześnie technika mikropunktów (wykonywanych nawet w tysiącach sztuk w technice grawerowania laserowego) jest ciągle wykorzystywana, także komercyjnie np. do zabezpieczania żetonów w kasynach przed podrabianiem, znakowania samochodów lub cennych przedmiotów (Piekałkiewicz, 1999).

2.2 KRYPTOGRAFIA SYMETRYCZNA – TECHNIKI „KLASYCZNE"

Ciekawostką jest, że jedna z prawdopodobnie najstarszych metod szyfrowania wykorzystywała urządzenie szyfrujące – było to spartańskie *scytale* z V wieku p.n.e. (Singh, 2003).

Metoda ta polegała na nawinięciu na kij lub walec o określonej grubości długiego paska materiału i napisaniu wzdłuż jego osi wiadomości. Pozostałą część pergaminu pokrywano dowolnymi literami. Właściwe odczytanie wiadomości było w zasadzie możliwe tylko przy użyciu kija lub walca o tej samej grubości. Dodatkowo, goniec mógł dostarczyć wiadomość do adresata wykorzystując m.in. steganograficzne sztuczki, np. opasując się listem, literami do ciała.

Scytale zostało przedstawione na fotografii 2.1.

Warto zauważyć, że idea szyfrowania wiadomości w oparciu o scytale była wykorzystywana także w czasach nowożytnych. Przykładem może być tutaj tzw. dysk Jeffersona (Fot. 2.2.), czyli urządzenie składające się z dysków, wokół których w losowy sposób rozłożone są litery alfabetu. Obecnie przyjmuje się, ze liczba dysków powinna odpowiadać liczbie liter w alfabecie angielskim – 26 – jednak można spotkać urządzenia z mniejszą (np. 10) lub większą (np. 30) liczbą dysków.

Wynalezienie dysku Jeffersona przypisuje się Thomasowi Jeffersonowi, jednak w ówczesnych czasach (koniec XVIII w.) urządzenie to nie osiągnęło zbyt dużej

popularności. Warto jednak zauważyć, że podobne rozwiązania istniały już wcześniej, m.in. piętnastowieczny kryptograf obrotowy, opracowany przez Leone Battistę Albertiego (Kahn, 1997).

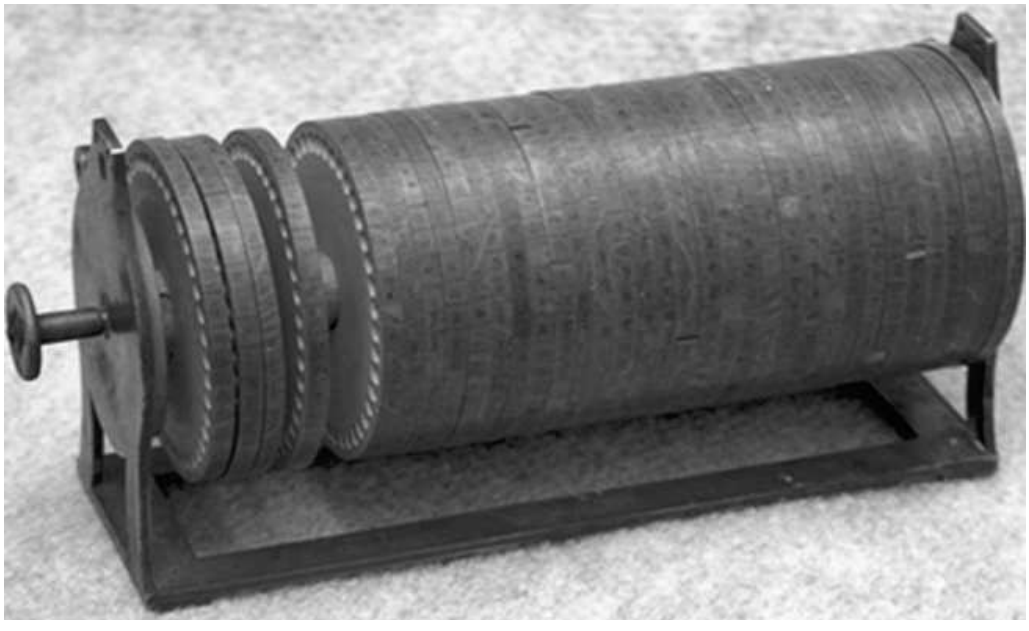
Uznanie zdobyło jednak dopiero urządzenie opracowane w 1890 roku przez francuskiego kryptologa Étienne Bazeriesa. W latach 1923-1942 dysk Jeffersona był wykorzystywany w armii Stanów Zjednoczonych jako urządzenie szyfrujące M-94 (Kahn, 1997).

Urządzenie składa się z umieszczonych obok siebie dysków, z nadrukowanymi literami alfabetu (na każdym w inny, losowy sposób), które można obracać niezależnie od siebie.

Osoba chcąca zaszyfrować wiadomość musi ułożyć z liter na dyskach tekst jawny, a następnie podać którykolwiek z pozostałych wierszy jako wiadomość.

Odbiorca wiadomości, znając kolejność ułożenia dysków oraz szyfrogram, może odszyfrować właściwą wiadomość, przeglądając tekst, jaki tworzą poszczególne wiersze – tylko jeden z wierszy powinien zawierać tekst zrozumiały dla człowieka. Podwójną rolę – klucza szyfrującego i wiadomości pełni tu kolejność w jakiej zostały ułożone dyski (Kahn, 1997).

Fot. 2.1. Scytale – współczesna rekonstrukcja
(źródło: Luringen, 2012)



Fot. 2.2. Dysk Jeffersona
(źródło: NSA, 2012)

Interesującą wariacją scytale może być również współczesny szyfr płotkowy. Kluczem jest tutaj wysokość płotka, czyli ilość rzędów, w jakich zapisywane są litery. Poniższy schemat pokazuje zaszyfrowanie tekstu LASKOWSKI MACIEJ przy użyciu płotka o wielkości 5.

L								I						
	A						K		M					
		S				S				A				J
			K		W						C		E	
				O								I		

Poszczególne litery szyfrogramu odczytywane są rzędami.

Tak więc szyfrogram to: `LIAKMSSAJKWCEOI`.

Odszyfrowanie polega na ponownym zapisaniu szyfrogramu w płotku o tej samej wysokości.

2.2.1 METODY PODSTAWIENIOWE

Jeden z najstarszych opisów szyfrowania znajduje się w *Kamasutrze*, dziele napisanym w IV wieku przez bramińskiego uczonego Vatsyayana, który korzystał z rękopisów pochodzących nawet z IV w p.n.e. *Kamasutra* zaleca kobietom poznanie 64 sztuk, takich jak gotowanie, ubieranie się, masaż i przygotowanie perfum.
Na liście tej znajdują się również inne sztuki, takie jak wróżbiarstwo, gra w szachy, introligatorstwo i stolarka, natomiast pozycja numer 45 to *mlecchita-vikalpa*, sztuka posługiwania się tajnym pismem, która ma pomóc kobietom w ukryciu swoich związków (Byrski, 1985).
Jedna z zalecanych metod polega na losowym połączeniu liter alfabetu w pary, a następnie zastąpieniu w jawnym tekście kolejnych liter przez litery z danej pary. Przykładowo, zestawiając znaki alfabetu łacińskiego w następujące pary:

L	A	S	K	O	W	I	G	D	R	U	Z	Y
M	C	E	J	B	F	H	N	P	T	W	X	Q

wiadomość *SPOTKAJMY SIE O POLNOCY* można zapisać jako *EDBRJCKLQ EHS B DBMGBAQ.*

Powyższa metoda szyfrowania nazywana jest **szyfrem podstawieniowym**. Każda litera w tekście jawnym jest zastępowana (podstawiana) inną literą.

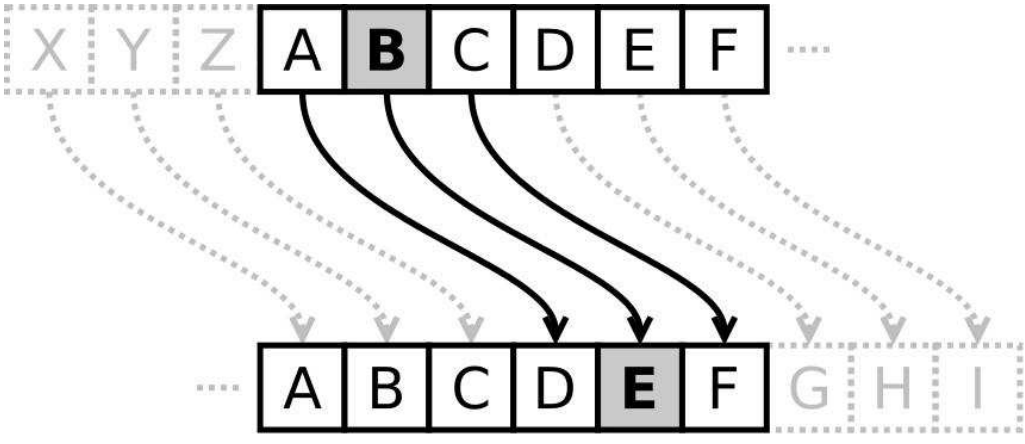
Szyfr Cezara

Za najstarszy, udokumentowany historycznie przykład zastosowania szyfru podstawieniowego uznaje się list Cezara do jego legata, Kwintusa Cycerona. Podstawienie polegało na zastąpieniu rzymskich liter greckimi, co sprawiło, że tekst stał się niezrozumiały dla nieprzyjaciela (Singh, 2003).

Cezar posługiwał się tajnym pismem tak często, że Waleriusz Probus napisał cały traktat o jego szyfrach, który niestety nie przetrwał do naszych czasów (Singh, 2003).

Jednak jego najsłynniejszy szyfr monoalfabetyczny (czyli używający jednego alfabetu podstawieniowego) przetrwał do dzisiejszych czasów dzięki *Żywotom*

Cezarów Swetoniusza z II wieku n.e. Szyfr Cezara (bo pod taką nazwą przetrwał w historii) polegał na tym, że każdą literę w tekście jawnym zastępowano literą położoną trzy miejsca dalej w alfabecie – vide Rys. 4.3. (Trankwillus, 1960).



Rys. 2.3. Przykład zamiany liter w klasycznej formie szyfru Cezara (z przesunięciem o 3) (źródło: Garbarczuk & Świć, 2005)

Tak więc słynne słowa Cezara *alea iacta est* zostałyby zaszyfrowane jako *dohd ldfwd hvw*. Niestety, Cezar nie szyfrował w żaden sposób liczb, tak więc byłyby one podane tekstem całkowicie jawnym (Kahn, 1997).

Przed Cezarem jego adoptowany syn, Oktawian August, używał szyfru przesuwającego z przesunięciem o 1 (Singh, 2003).

Bezpieczeństwo szyfru przesuwającego w ówczesnych czasach jest nieznane. Należy jednak pamiętać, że w starożytności analfabetyzm był powszechny, zatem wielu wrogów Cezara mogło mieć kłopot z przeczytaniem samego tekstu, a co dopiero z rozkodowaniem go. Pierwsze udokumentowane metody łamania takich szyfrów autorstwa arabskiego filozofa Al-Kindi pochodzą z IX wieku, gdy zaczęto stosować analizę częstościową (Singh, 2003). Wraz z odkryciem tej techniki szyfr Cezara utracił swoją praktyczną wartość.

Obecnie ten algorytm szyfrowania nie zapewnia prawie żadnego bezpieczeństwa – liczba wszystkich możliwych kluczy deszyfrujących jest równa liczbie liter w alfabecie – czyli 26 (Singh, 2003).

Wystarczy więc wypróbować wszystkie, aby przekonać się, ze tylko jedna wiadomość będzie zawierać sensowny tekst, cała zaś reszta będzie tylko mniej lub bardziej przypadkową zbieraniną liter. Nie zmienia to jednak faktu, iż ciągle jest wykorzystywany (choć niekoniecznie w klasycznej – z przesunięciem o 3 – formie). Istotną rzeczą jest to, iż dwu-, albo i nawet trzykrotne szyfrowanie tekstu nie wpłynie zasadniczo na poziom jego bezpieczeństwa – np. szyfrując tekst najpierw z przesunięciem o 3 litery, a następnie o 12 liter uzyskamy taki sam efekt jak używając przesunięcia piętnastoliterowego (Abramson, 1963).

Szyfr Cezara z przesunięciem 1 w lewo zastosowany został na odwrocie mezuz do zakodowania hebrajskich imion Boga (zapisanych po odwróceniu pergaminu o 180°, by zachowana została kolejność liter po drugiej stronie). Na pergaminie widnieje szyfrogram *KUZU BMUKSZ KUZU*, co po odkodowaniu (w alfabecie hebrajskim) daje *YHVH ELHYNU YHVH*.
Uznaje się, że jest to pozostałość czasów, gdy Żydom nie pozwalano na posiadanie mezuzy. Natomiast same litery kryptogramu zawierają boskie imię, co miało chronić przed złymi mocami (Półtorak, 2012).

W XIX wieku gazetowe rubryki ogłoszeń drobnych były często wykorzystywane do przekazywania zaszyfrowanych prostymi kodami wiadomości, zwłaszcza tych dotyczących relacji damsko-męskich (Kahn, 1997).

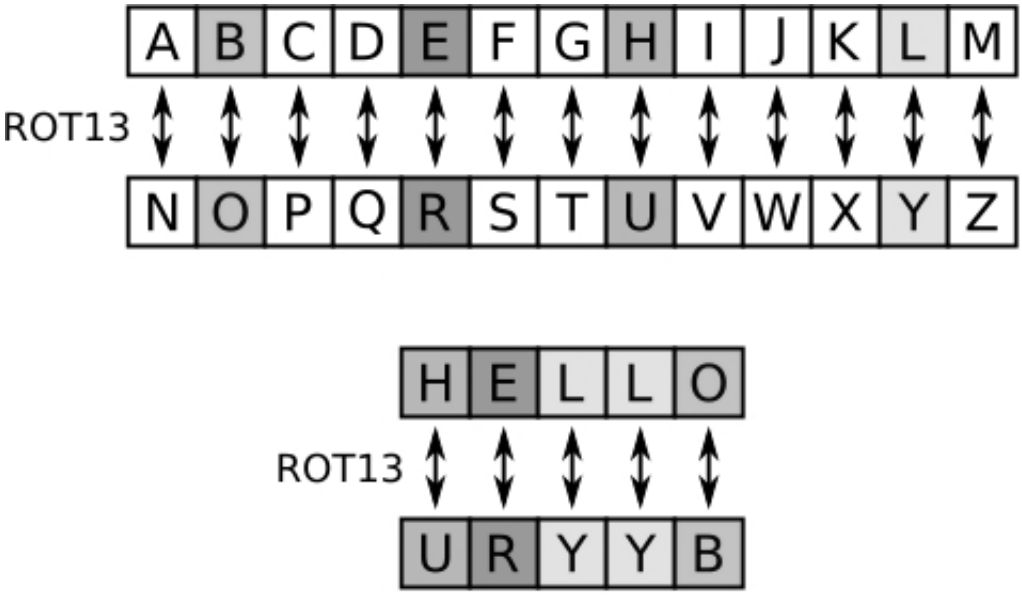
Szyfr Cezara był używany podobno jeszcze w czasie I Wojny Światowej przez armię rosyjską, gdyż tylko taki szyfr wydawał się być zrozumiały dla większości oficerów sztabowych. Dzięki temu niemieccy i austriaccy kryptoanalitycy nie mieli większych problemów z odczytaniem rosyjskich wiadomości (Kahn, 1997).

W kwietniu 2006 roku szef mafii Bernardo Provenzano został schwytany na Sycylii częściowo dzięki kryptoanalizie jego wiadomości zakodowanych odmianą szyfru Cezara. Provenzano do szyfrowania używał liczb, zastępując literę „A" cyfrą „4", „B" – „5" itd. (Leyden J. , 2006).

Co ciekawe szyfr Cezara przeżył na przełomie lat 80. i 90.-tych XX wieku drugą młodość – jako ROT-13. Ta metoda szyfrowania (zastąpienie litery tekstu jawnego literą występującą 13 pozycji dalej – vide Rys. 2.4.) używana była w Usenecie i w środowisku Unixowym – bynajmniej jednak nie do zachowania tajemnicy.

Za pomocą ROT-13 szyfrowano zazwyczaj teksty lub wyrazy niecenzuralne lub zabronione przez moderatora (np. spoilery) – robiono to jednak tak, aby osoba, która tego chce, mogła je odczytać (stąd prostota szyfru). Ponad to ROT-13 miał jeszcze jedna ważną zaletę – tak zaszyfrowany tekst przechodził przez wszystkie filtry wyszukujące niedozwolone słowa lub frazy. Dopiero późniejsze wersje filtrów umiały sobie poradzić z tak prostym szyfrem.

Niemniej jednak ciągle jeszcze na niektórych grupach usenetowych używa się wyrazów zapisanych ROT-13 (Wobst, 2001).



Rys. 2.4. Przykład działania szyfru ROT-13
(źródło: Esham, 2012)

Jako ciekawostkę należy podać, że dla niektórych wyrażeń w języku polskim (o ile nie są użyte polskie znaki diakrytyczne) kodowanie ROT-13 nie spełnia swojego zadania.

Przykładowo, tekst *hejnal urwany* po zakodowaniu brzmi *urwany hejnal*.

Atbasz

Atbasz to tradycyjna hebrajska odmiana szyfru podstawieniowego. Szyfr ten polega na zastąpieniu litery położonej w pewnym miejscu, licząc od początku alfabetu, literą położoną w takim samym miejscu, licząc od końca. W przypadku alfabetu łacińskiego oznaczałoby to, że „A" jest zastąpione przez „Z", „B" przez „Y" i tak dalej.

Sama nazwa Atbasz wskazuje na schemat podstawiania, ponieważ składa się z pierwszej litery hebrajskiego alfabetu – *alef*, po której następuje ostatnia – *taw*, dalej mamy drugą literę *beth*, a po niej przedostatnią *shin* (Garbarczuk & Świć, 2005).

Przykładem zastosowania szyfru Atbasz w Starym Testamencie można znaleźć w *Księdze Jeremiasza*, wersety 25:26 i 51:41, w którym słowo *Babilon* (*Babel*) jest zastąpione słowem *Szeszak*. Dwie litery *beth* (druga literą hebrajskiego alfabetu) zostały zastąpione literami *shin*. Ostatnia litera Babel to *lamed*, dwunasta litera alfabetu – została ona zastąpiona *kaph*, dwunastą literą od końca.

Ponowne zaszyfrowanie tekstu jest równoznaczne z jego odszyfrowaniem.

Szyfr podstawieniowy z własnym alfabetem szyfrowym

Pomimo swojej prostoty szyfr Cezara stanowił źródło inspiracji dla przyszłych pokoleń kryptologów.

Jak zostało już wspomniane, system kryptograficzny dopuszczający niewiele kluczy nie jest bezpieczny i stosunkowo łatwo jest go złamać.

Jednym z prostszych sposobów zapewnienia bezpieczeństwa wydaje się być zwiększenie liczby kluczy – rozwiązaniem opartym o to rozumowanie jest szyfr opracowany przez szesnastowiecznego uczonego Girolamo Cardano (Kahn, 1997).
Metoda ta opiera się o przyporządkowanie każdej literze alfabetu łacińskiego innej, według dowolnie wybranego klucza – na przykład według układu klawiatury:

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
Q W E R T Y U I O P A S D F G H J K L Z X C V B N M

Tak więc słynne słowa Cezara *alea iacta est* zostaną teraz zaszyfrowane jako *qstq oqezq tlz*.

Metoda Cardano charakteryzuje się ogromną liczbą potencjalnych kluczy. W przypadku alfabetu opartego o 26 liter liczba ta wynosi 26!, czyli 403291461126605635584000000 (Guzicki, 1997). Pozornie więc wydaje się być praktycznie nie do złamania.

Równolegle stopniowo udoskonalano metody podstawieniowe – np. alfabet łaciński zastępowano innym, stworzonym przez szyfrującego, niekoniecznie opartym na „zwykłych" literach (Kahn, 1997).

Tego typu szyfry są popularne do dzisiaj – gdyż dla laika wydają się być nie do złamania podobnie, jak szyfr Cardano.

Jednak opisane powyżej metody kryptograficzne (zarówno Cardano, jak i szyfry podstawieniowe oparte o własny alfabet) w rzeczywistości bardzo łatwo jest zdekodować, posługując się w tym celu metodą statystycznej analizy występowania znaków, czyli mówiąc prościej badając częstotliwość występowania liter w tekście (Schneier, 2002).

Tabela 2.1. zawiera zestawienie częstotliwości występowania poszczególnych liter w języku polskim oraz angielskim, przy założeniu, że alfabet angielski liczy 26 liter, zaś alfabet polski – 32 litery (pomimo, iż nie ma potrzeby stosowania w polskim słowotwórstwie liter takich jak „V", „Q" czy „X", to występują one w wyrazach pochodzenia obcego).

Dodatkowo, tabela dla alfabetu polskiego została również opracowana w wersji 26-literowej, bez polskich znaków diakrytycznych (czyli litery „A" i „Ą", „C" i „Ć" „E" i „Ę", „L" i „Ł", itd. traktowane są jako jedna i ta sama).

Analizując poniższą tabelę nie należy zapominać o tym, iż istnieją również znaki występujące w tekście pisanym częściej, niż litery – jest to m.in. spacja, znaki przestankowe czy – występujący często w języku angielskim – pojedynczy apostrof (‘). Należy mieć to na uwadze dokonując analizy częstotliwościowej tekstu.

język				
polski			angielski	
litera	częstotliwość występowania (%)		litera	częstotliwość występowania (%)
	pełny alfabet (32 litery)	alfabet bez polskich znaków diakrytycznych (26 liter)		
A	8,91	9,90	E	12,702
I	8,21	7,16	T	9,056
E	7,66	8,77	A	8,167
O	7,75	6,75	O	7,507
Z	5,64	6,53	I	6,966
N	5,52	5,72	S	6,749
W	4,65	4,65	N	6,327
S	4,32	4,98	H	6,094
R	4,69	4,69	R	5,987
Y	3,76	3,76	D	4,253
C	3,96	4,36	L	4,025
T	3,98	3,98	U	2,782
D	3,25	3,25	M	2,758
M	2,80	2,80	C	2,406
K	3,51	3,51	F	2,360
P	3,13	3,13	G	2,228
J	2,28	2,28	W	2,015
U	2,50	2,50	Y	1,974
L	2,10	2,10	P	1,929
B	1,47	1,47	B	1,492
Ę	1,11	-	K	0,978
G	1,42	1,42	V	0,772
Ą	0,99	-	J	0,153
H	1,08	1,08	X	0,150
Ż	0,83	-	Q	0,095

język				
polski			angielski	
litera	częstotliwość występowania (%)		litera	częstotliwość
Ś	0,66	-	Z	0,074
Ó	0,85	-		
Ć	0,40	-		
F	0,30	0,30		
Ń	0,20	-		
Ź	0,06	-		
V	-	-		
Q	-	-		
X	-	-		

Tab. 2.1. Częstotliwość występowania poszczególnych liter w języku polskim i angielskim (źródło: opracowanie własne na podstawie (KorpusPAN, 2012) oraz (OxfordDictionary, 2012)

Propagatorem metody analizy częstotliwościowej w tzw. kulturze masowej był dziewiętnastowieczny amerykański pisarz Edgar Allan Poe, który pokazał jej działanie w swoim opowiadaniu pt. *Złoty żuk* z 1843 roku.

Bohaterowie tej opowieści natrafiają na tajemniczą wiadomość o następującej treści (za: Poe, 2012):

53QQ+305)6x;4826)4Q);48+8I60)85;1Q(;:Qx8+83(88)5x+
;46(;88x96x?;8)xQ(;485);5x+2:xQ(;4956x2(5x-
4)8I8x;4069285);)6+8)4QQ;1(Q9;48081;8:8Q1;48+85;4)
485+528806x81(Q9;48;(88;4(Q?34;48)4Q;161;:188;Q?;

Bohaterowie Poego znają podstawy analizy statystycznej – wiedzą na przykład, że najczęściej używaną literą w języku angielskim jest „*e*", zaś najczęściej używanym wyrazem – „*the*".

Analizując treść szyfrogramu zauważają, że dość często powtarza się tam ciąg *;48* – przypisują więc tym trzem znakom odpowiednie litery. Podstawiając uzyskane znaki do szyfrogramu zauważają, że występuje w nim ciąg *;Q88* – co odpowiada wyrazowi

tree. W ten sposób uzyskują kolejny znak, który podstawiają do tekstu i tak dalej, aż co całkowitego jego rozszyfrowania.

Ostatecznie wiadomość prowadząca do skarbu kapitana Kidda po podzieleniu na wyrazy brzmi (za: Poe, 2012):

A good glass in the bishop's hostel in the devil's seat – forty-one degrees and thirteen minutes – northeast and by north main branch seventh limb east side shoot from the left eye of the death's-head a bee-line from tree through the shot fifty feet out.

(Dobre szkła w hotelu biskupa na siedzeniu diabła – czterdzieści jeden stopni i trzynaście minut – północny-wschód i na północ główny pień siódmy konar od wschodu spuścić z lewego oka trupiej czaszki linię prostą od drzewa przez kulę piętnaście stóp dalej).

Opowiadanie Poe odegrało znaczącą rolę w popularyzacji kryptogramów w gazetach i czasopismach w drugiej połowie XIX wieku. Stanowiło również źródło inspiracji dla kolejnych pokoleń kryptologów i kryptoanalityków – William Friedman zainteresował się kryptografią po przeczytaniu *Złotego żuka* jeszcze jako dziecko i owe zamiłowanie wykorzystał potem deszyfrując japońską maszynę szyfrującą Purple podczas II wojny światowej (Rosenheim, 1997). Analogiczna sytuacja miała miejsce w przypadku polskiego kryptologa, Jana Kowalewskiego (vide Rozdz. 2.4.4).

Również najsłynniejszy detektyw świata, Sherlock Holmes, musiał zmierzyć się z analizą statystyczną, aby odszyfrować tajną wiadomość. W opowiadaniu *Tańczące sylwetki* Holmes po złamaniu kodu (w którym rolę alfabetu pełnią tytułowe tańczące sylwetki (Rys. 2.5), wysyła sfałszowaną wiadomość do jednego z bohaterów opowieści, dzięki czemu jest w stanie zwabić go w pułapkę i udowodnić jego winę.

Rys. 2.5. Tańczące sylwetki z opowiadania o Sherlocku Holmesie (źródło: Doyle, 2011)

Utrudnieniem dla kryptoanalityków może być użycie oprócz alfabetu szyfrowego także tzw. **nomenklatora**, czyli krótkiej listy słów (lub znaków) kodowych, mających zastępować określone wyrazy tekstu jawnego.

Szyfry oparte o nomenklatory są możliwe do złamania. Nie odbywa się to jednak przy pomocy prostej analizy częstościowej znaków, ale przy pomocy analizy częstości grup znaków – digramów i trigramów (Kahn, 1997).
Wadą książek kodowych jest również to, że w razie wpadnięcia w ręce wroga wszystkie przechwycone wcześniej depesze były łatwe do rozszyfrowania.

Historia Marii Stuart jest jedną z najbardziej znanych opowieści związanych z kryptografią i kryptoanalizą, zarówno ze względu na tło historyczne, jak i na konsekwencje, jakie przyniosło złamanie szyfru, jakim posługiwała się szkocka władczyni, pomimo używania nomenklatora, uważanego wówczas za nie do złamania. Dodatkowo historia ta pokazuje drogę, jaką przebyły techniki ochrony informacji od czasów antycznych, a więc na przestrzeni prawie dwóch tysięcy lat.

Po przegranej w bitwie pod Langside Maria I Stuart, królowa Szkocji, uciekła do Anglii, gdzie została uwięziona w Carlisle przez wojska Elżbiety I, królowej Anglii.
Po prawie 18 latach uwięzienia, w 1586 roku, Maria otrzymała pakiet listów, które pochodziły od jej zwolenników na kontynencie. Do więzienia przemycił je Gilbert Gifford, który wyjechał z Anglii w 1577 roku i kształcił się na księdza w angielskim kolegium w Rzymie, zaś po powrocie do Anglii w 1585 roku chcąc służyć Marii rozpoczął rolę kuriera – nie tylko przekazywał listy do niej, ale również odbierał jej odpowiedzi. Do transportu listów wykorzystywał metody steganograficzne – zanosił bowiem listy do lokalnego piwowara, który owijał je w skórę i umieszczał je w wydrążonym drewnianym szpuncie od beczki z piwem. Piwowar dostarczał beczkę do Chartley Hall, gdzie jeden ze służących Marii otwierał szpunt i zanosił jego zawartość do królowej Szkocji. Ten sam mechanizm pozwalał również wynosić listy z twierdzy (Singh, 2003).

W tym samym czasie, bez wiedzy Marii, w jednej z londyńskich tawern narodził się plan jej wyzwolenia. Głównym inicjatorem spisku był Anthony Babington, którego wobec władzy była więc uzasadniona względami religijnymi, a pomoc dla Marii, przeciwniczki Elżbiety, była jednym ze sposobów walki z angielską władzą.

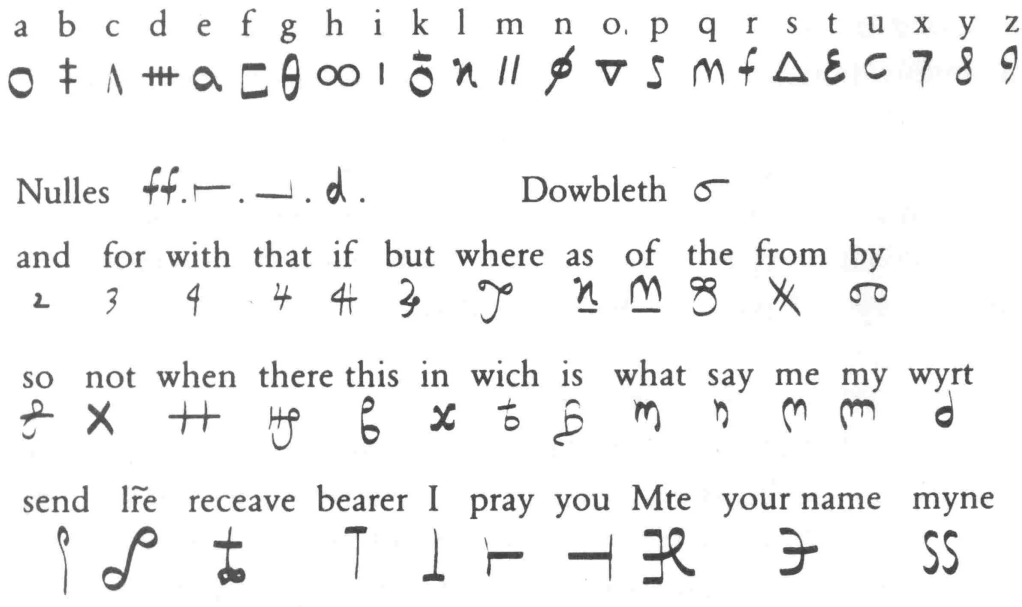
Spisek został zawiązany w marcu 1586 roku. W ciągu kilku miesięcy spiskowcy ułożyli plan: zamierzali uwolnić Marię Stuart, zamordować królową Elżbietę i wzniecić bunt, wspomagany przez zagraniczne wojska (Kahn, 1997).

Konspiratorzy uważali, że spisek wymaga poparcia Marii, ale nie wiedzieli, w jaki sposób się z nią skontaktować. Wówczas do Babingtona przyjechał Gifford, przywożąc list od Marii, w którym królowa pisała, że słyszała o Babingtonie od swoich zwolenników w Paryżu i oczekuje na wiadomość od niego. W odpowiedzi Babington szczegółowo przedstawił swój plan (za: Donaldson, 1974):

Osobiście z dziesięcioma innymi szlachcicami i setką naszych zwolenników podejmę się uwolnienia Waszej Królewskiej Mości z rąk nieprzyjaciół. Jesteśmy uwolnieni od obowiązku posłuszeństwa wobec uzurpatorki, gdyż została ona ekskomunikowana. Jej usunięciem zajmie się sześciu znakomitych szlachciców, moich najzaufańszych przyjaciół, którzy – z gorliwości w służbie katolickiej sprawy i Waszej Królewskiej Mości – chcą ów zamach wykonać.

Gifford ponownie ukrył wiadomość w szpuncie od beczki z piwem, by przemycić list do więzienia Marii. Jednak, zdając sobie sprawę z niebezpieczeństwa przechwycenia listu, Babington zaszyfrował wiadomość do królowej nie zwykłym szyfrem monoalfabetycznym, lecz szyfrem podstawieniowym opartym o nomenklator, w którym litery i niektóre zwroty zostały zastąpione symbolami (Singh, 2003). Nomenklator ten przedstawiony został na rysunku 2.6.

Jednak Gilbert Gifford, który zajmował się transportem listów między Marią a spiskowcami, był podwójnym agentem, pracującym dla Sir Francisa Walsinghama – ministra dworu angielskiego, pełniącego również obowiązki szefa wywiadu, odpowiedzialnego za bezpieczeństwo monarchini, Elżbiety I (Singh, 2003). Ilekroć Gifford odbierał list do lub od Marii, najpierw zanosił go do Walsinghama, który przekazywał go fałszerzom, którzy łamali pieczęć, kopiowali list, po czym pieczętowali go ponownie przy pomocy podrobionego stempla. Następnie Gifford zabierał pozornie nienaruszony list i dostarczał list Marii lub jej korespondentom (Singh, 2003).



Rys. 2.6. Nomenklator używany przez szkocką królową Marię I Stuart (źródło: Singh, 2003)

Oczywiście samo skopiowanie wiadomości nie dawało żadnego rezultatu – należało bowiem jeszcze złamać szyfr. Zdając sobie sprawę z wartości kryptoanalizy, Walsingham założył w Londynie własną szkołę szyfrów i zatrudnił tam na stanowisku sekretarza Thomasa Phelippesa (Singh, 2003). Dzięki analizie statystycznej udało się rozpoznać wszystkie symbole alfabetu szyfrowego i słowa kodowe.

Odszyfrowanie listów ukazało powagę sytuacji – gdy odszyfrowano wiadomości, w których spiskowiec w jawny sposób proponował zamordowanie Elżbiety, Walsingham mógł już aresztować Babingtona, jednak postanowił poczekać, aż Maria odpowie i zaaprobuje spisek (Singh, 2003).

Maria odpowiedziała Babingtonowi, nalegając, by uwolniono ją przed lub równocześnie ze zgładzeniem Elżbiety. Bała się bowiem, że gdyby wiadomość o śmierci królowej dotarła do jej strażnika, ten mógłby ją zamordować (Singh, 2003).

Walsingham miał już wystarczające dowody, by aresztować Babingtona i Marię, wciąż jednak aby całkowicie zniweczyć spisek, potrzebował nazwisk pozostałych konspiratorów.

Dlatego polecił Phelippesowi, aby sfałszował postscriptum (Fot. 2.7) do listu Marii, które nakłoniłyby Babingtona do podania nazwisk (za: Donaldson, 1974):

Chciałabym poznać nazwiska i zalety sześciu szlachciców, którzy mają wykonać zadanie – może się bowiem okazać, że będę w stanie, po poznaniu uczestników, dać Panu dodatkowe rady, z jakich należy przy tym skorzystać, a w szczególności również jak postępować dalej.

Chciałabym jak najszybciej wiedzieć, w tym samym celu, kto już i w jakim stopniu jest w to wtajemniczony.

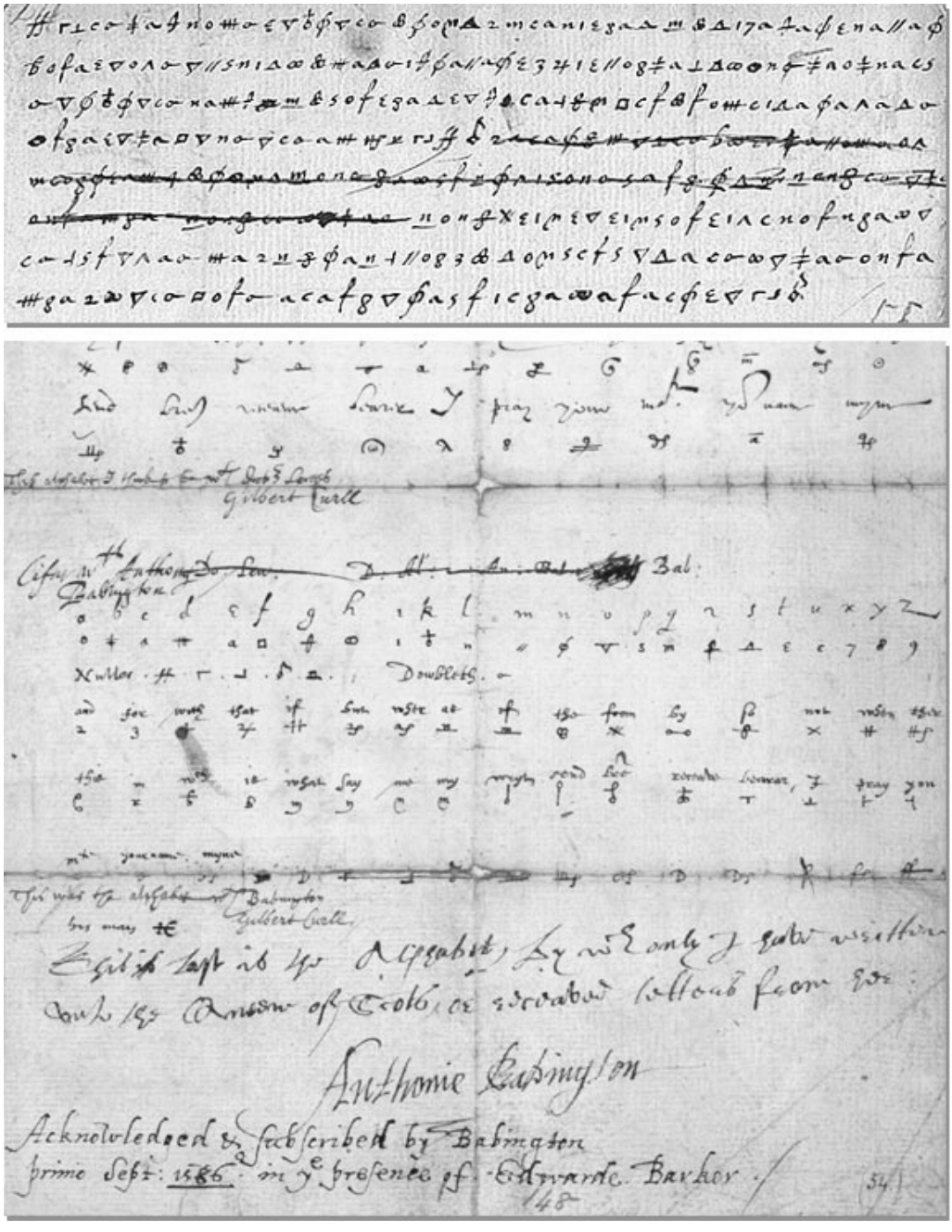
List ten dowodzi, że szyfr złamany przez podsłuchującego jest gorszy od braku szyfru. Zarówno Maria Stuart, jak i Babington pisali szczegółowo o swoich zamiarach, sądząc, że ich listy są bezpieczne. Ponadto ich zaufanie do szyfru sprawiło, że Babington zaakceptował fałszerstwo Phelippesa.

Wkrótce po otrzymaniu listu z postscriptum, Babington wraz ze swoimi sześcioma wspólnikami został złapany i sprowadzony do Londynu. Zdrajców natychmiast osądzono i skazano na kary śmierci (Donaldson, 1974).

Sama Maria została oskarżona o udział w spisku przeciwko życiu królowej Elżbiety. Postępowanie rozpoczęło się przed komisją składającą się z dwóch głównych sędziów i czterech ławników, w obecności m.in. Walsinghama, Phelippesa oraz wielu lordów i baronów. Obrona królowej polegała na wypieraniu się wszelkich związków z Babingtonem. Ta deklaracja wobec zgromadzonych dowodów nie miała jednak znaczenia: Izba Gwiaździsta na posiedzeniu w Westminsterze oświadczyła, że Maria jest winna układania i planowania zdarzeń zmierzających do śmierci królowej Anglii oraz zaleciła karę śmierci (Singh, 2003). Elżbieta I podpisała wyrok, który został wykonany 8 lutego 1587 (Donaldson, 1974).

Szyfr polialfabetyczny

W swojej najsłynniejszej, opublikowanej w 1586 roku pracy *Traicte des Chiffres* francuski uczony Blaise de Vigenère przedstawił wiele odmian starego systemu polialfabetycznego zwiększając ich złożoność za pomocą trudniej przewidywalnych tabel oraz *autokluczy* – w przypadku których sam tekst jawny był kluczem szyfrującym.



Fot. 2.7. Sfałszowane postscriptum (na górze rysunku) oraz nomenklator używany przez Babingtona
(źródło: SP12/193/54 oraz SP53/18/55)

System Vigenère'a zyskał trwałą reputacje bezpiecznego – był znany jako *le chiffre indechiffrable*. Stosowano go jeszcze na początku dwudziestego wieku jako niezbędny składnik systemów szyfrowania (Kahn, 1997).

Szyfr Vigenère opierał się o opracowaną przez Johannesa Trithemiusa tzw. *tabela recta,* czyli tablicę alfabetów, w której każdy wiersz był przesunięty o jeden znak w lewo.

Sposób działania szyfru Vigenère można przedstawić następująco: odbiorca wraz z nadawcą ustalają hasło stanowiące podstawę klucza, które następnie umieszczają pod tekstem jawnym – jeśli jest ono krótsze od tego tekstu, to jest ono powtarzane odpowiednią ilość razy.

Kolejną czynnością jest zaszyfrowanie każdego znaku – każda litera tekstu jawnego jest zastępowana odpowiednią literą z alfabetu, rozpoczynającego się od przypisanej mu litery hasła.

Nieznajomość hasła oraz kolejności liter w przyjętych alfabetach przez osoby postronne sprawia, iż liczba kluczy wzrasta wielokrotnie.
W przypadku tzw. *autoklucza* ustalana jest jedynie pierwsza litera klucza – kolejnymi jego literami są kolejne litery tekstu jawnego.

Poniżej zaprezentowany został przykład szyfrowania tekstu metodą Vigenère z *autokluczem*, gdzie pierwszą literą klucza jest litera M.

tekst jawny:	`LASKOWSKI MACIEJ`
klucz:	`MLASKOWSK IMACIE`
tekst zaszyfrowany:	`XLSCYKOCS UMCKMN`

Odszyfrowanie wiadomości zaszyfrowanej za pomocą szyfru Vigenère przebiega w następujący sposób: pierwsza litera szyfrogramu odszyfrowywana jest za pomocą ustalonej pomiędzy stronami litery, zaś kolejne litery szyfrogramu za pomocą dopiero co odcyfrowywanych liter.

Bazując na powyższym przykładzie:

tekst jawny:	XLSCYKOCS UMCKMN
klucz:	MLASKOWSK IMACIE
tekst zaszyfrowany:	LASKOWSKI MACIEJ

Tablica, na której Vigenère oparł swój szyfr została przedstawiona w tabeli 2.2.

Szyfr Vigenère opierał się prostej analizie statystycznej głównie ze względu na fakt, iż długość klucza była równa długości tekstu jawnego (w razie potrzeby klucz powtarzano odpowiednią ilość razy, jak na powyższym przykładzie).

Ciekawą techniką (poza autokluczem) jest również wykorzystanie tzw. klucza ciągłego, czyli fragmentu tekstu, np. książki, którego długość będzie równa długości tekstu jawnego, a jednocześnie klucz ten nie będzie się powtarzał.

Pierwszy opis złamania szyfru Vigenère autorstwa pruskiego dowódcy Fryderyka Kasiskiego został opublikowany w 1863 (Kasiski, 1863).

Metoda ta jednak została opracowana już wcześniej – około roku 1854 – przez Charlesa Babbage, który odszyfrował tekst wiersza *Wizja grzechu* autorstwa Alfreda Tennysona zaszyfrowany przy pomocy słowa-klucza *emily* (imię żony Tennysona). Babbage nie ujawnił sposobu w jaki tego dokonał, jednak analiza jego notatek pozwoliła na stwierdzenie, że posłużył się tym samym sposobem co Kasiski (Franksen, 1985).

Metoda opierała się o obserwację, że powtórzenia w szyfrogramie mogą odpowiadać powtórzeniom w tekście jawnym i kluczu. To z kolei ułatwiało odgadnięcie długości klucza, zaś następnie samego klucza i odszyfrowania szyfrogramu (Kasiski, 1863).

Oczywiście metoda ta dotyczyła historycznej wersji szyfru Vigenère, która miała skończoną (i w praktyce zazwyczaj krótką) długość klucza.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Tab. 2.2. Tabela Vigenère
(źródło: Singh, 2003)

Homofoniczny szyfr podstawieniowy

Ciekawym przykładem walki kryptologów z kryptoanalitykami jest homogeniczny szyfr podstawieniowy, którego schemat działania można opisać następująco: każdej literze alfabetu jawnego odpowiada kilka symboli alfabetu szyfrowego. Liczba możliwości jest proporcjonalna do częstości występowania danej litery.

Jak wynika z tabeli 2.1. w języku angielskim litera „a" teoretycznie występuje raz na osiem liter. W związku z tym, w homofonicznym szyfrze podstawieniowym przypisuje się tej literze osiem symboli – i ilekroć w tekście jawnym pojawi się „a", jest ona zastępowana symbolem wybranym losowo z ośmiu możliwych symboli. Dzięki temu w tekście zaszyfrowanym każdy symbol pojawia się w przybliżeniu z taką samą częstością – stanowi 1% wszystkich symboli tekstu.

Zgodnie z danymi z tabeli 2.1. w języku angielskim każdej literze odpowiada więc od jednego do dwunastu symboli, zależnie od częstości występowania tej litery (vide Rys. 2.8).

Każda dwucyfrowa liczba odpowiadająca literze „a" w tekście jawnym reprezentuje ten sam znak/dźwięk w tekście zaszyfrowanym – stąd nazwa szyfr homofoniczny (z greckiego: *homos* – 'ten sam', *phone* – 'dźwięk'.

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
09	48	13	01	14	10	06	23	32	15	04	26	22	18	00	38	94	29	11	17	08	34	60	28	21	02
12	81	41	03	16	31	25	39	70			37	27	58	05	95		35	19	20	61		89		52	
33		62	45	24			50	73			51		59	07			40	36	30	63					
47			79	44			56	83			84		66	54			42	76	43						
53				46			65	88					71	72			77	86	49						
67				55			68	93					91	90			80	96	69						
78				57										99					75						
92				64															85						
				74															97						
				82																					
				87																					
				98																					

Rys. 2.8. Przykład alfabetu szyfrowego dla homofonicznego szyfru podstawieniowego (źródło: Singh, 2003)

Jednym z najsłynniejszych szyfrów homofonicznych, wykorzystujący dodatkowo nomenklator był tzw. **Wielki Szyfr (Grande Chiffre)** opracowany przez ród francuskich kryptografów i kryptoanalityków, Rossignolów, których kilka pokoleń służyło francuskim królom. Protoplasta rodu, Antoine Rossignol złamał szyfr Huguenotów, użyty podczas oblężenia Réalmont do wysyłania wiadomości do sojuszników. Twierdza została zdobyta, gdy parlamentariusze pokazali dowódcy twierdzy rozszyfrowaną wiadomość z prośbą o zaopatrzenie i posiłki, którą wcześniej wysłał poza miejskie mury (Singh, 2003).

Po tym sukcesie Rossignolem zainteresował się kardynał Richelieu, który zdecydował się wykorzystać jego wiedzę i umiejętności do poprawy bezpieczeństwa informacji wysyłanych przez francuski rząd.

Owocem pracy Antoine Rossignol wraz z synem był opracowany na zlecenie Ludwika XIV *Le Grand Chiffre*, czyli Wielki Szyfr, który był wariacją szyfru homofonicznego z rozbudowanym nomenklatorem, łączył bowiem książkę kodów ze sporą tablicą podstawień homofonicznych, które dotyczyły zarówno liter, jak i całych wyrazów lub sylab.

Popularne wyrazy takie jak nazwiska znanych osób czy obiekty geograficzne (państwa, miasta, rzeki itd.) miały własne podstawienia homofoniczne.

Dodatkowo zastosowano pewne pułapki, jak chociażby „zerowe homofony", które niczego nie kodowały (po prostu pusty znak), a miały jedynie przeszkadzać w kryptoanalizie.

Inna pułapka to homofony, których wystąpienie „usuwało" pewien poprzedzający je rozszyfrowany fragment.

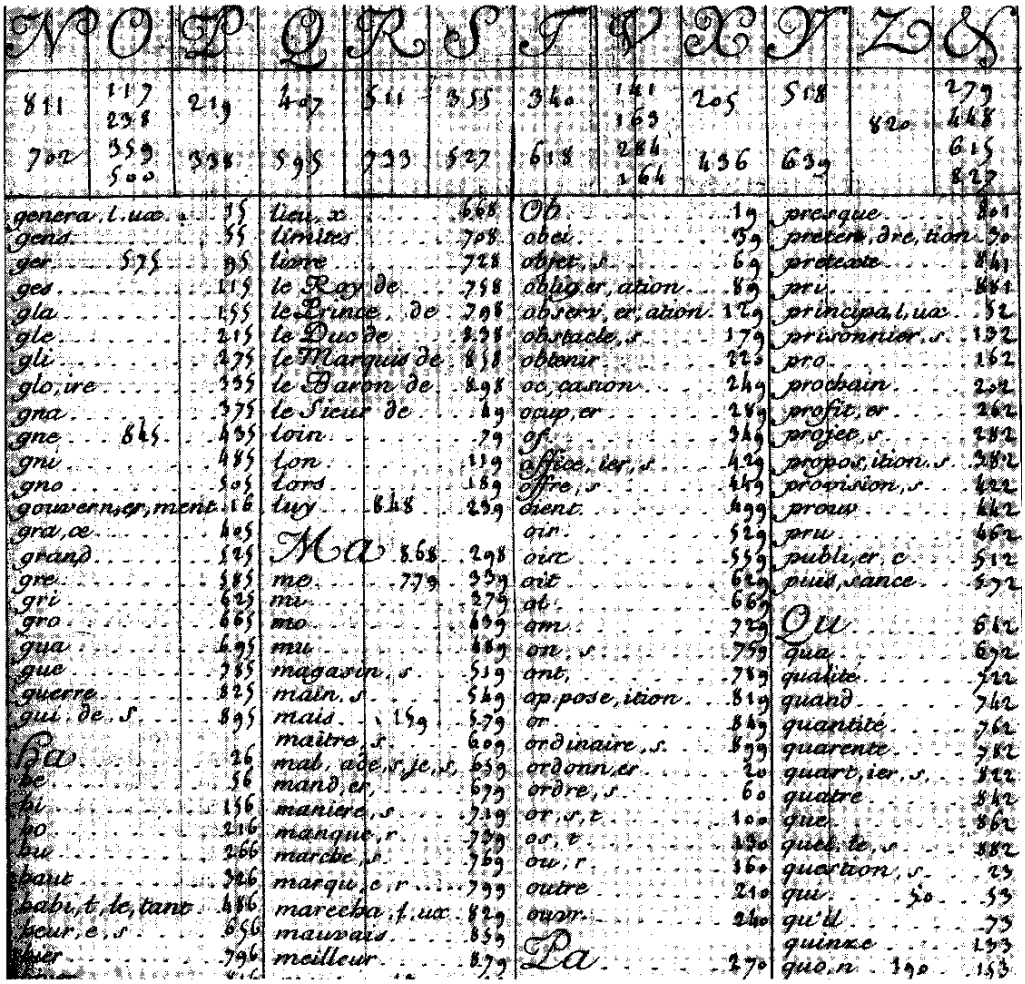
Dodatkowo, zabezpieczono się przed prostą analizą statystyczną – dowodem na to niech będzie fakt, że najpopularniejsza w języku francuskim litera „e" miała aż 131 homofonów z łącznej puli 711 występujących w całym szyfrze (Kahn, 1997).

O skuteczności Wielkiego Szyfru niech świadczy fakt, że nawet po tym, jak wyszedł z użycia (po śmierci Antoine-Bonaventure Rossignola) wiadomości zaszyfrowane przy jego pomocy pozostały niezłamane przez prawie trzysta lat, aż do XIX wieku, kiedy odczytał je Étienne Bazeries.

Jako ciekawostkę można podać fakt, że wykorzystał on do tego celu …analizę statystyczną. W jednym z analizowanych tekstów na każdej stronie pojawiała się kilkukrotnie sekwencja 124-22-125-46-345.

Bazieres słusznie założył, że odpowiada ona słowom *les ennemis* (les-en-ne-mi-s) (Singh, 2003).

Odkrycie to umożliwiło dalsze odszyfrowanie tekstu w oparciu o „zwykłą" analizę statystyczną.



Fot. 2.9. Fragment nomenklatora wykorzystywanego w Wielkim Szyfrze (źródło: Cryptologia, 2005)

Szyfr poligramowy

Szyfr Playfair został opracowany przez sir Charlesa Wheatstone w 1854 roku, zaś swoją nazwę zawdzięcza Lyonowi Playfair, pierwszemu Baronowi Playfair, który rozpropagował jego używanie.

Szyfr ten opiera się o tzw. *digramy* – czyli pary liter tekstu jawnego, które są zastępowane inną parą liter.

Aby zaszyfrować tekst przy użyciu szyfru Playfair należy najpierw stworzyć tabelę szyfrującą, opartą o jakieś słowo-klucz. W poniższym przykładzie będzie to MACIEJ. Jeśli w słowie-kluczu powtarzają się litery, to powtórzenia należy wyeliminować. Przykładowo: jeśli słowem-kluczem byłoby LASKOWSKI, to przyjęłoby ono formę LASKOWI.

Następnie poszczególne litery alfabetu zapisuje się (dla alfabetu angielskiego) w kwadracie 5x5 zaczynając od słowa kluczowego.

W celu dopasowania liczby liter do liczby pól pomija się literę „q" bądź też łączy się ze sobą w jednym polu litery „i" oraz „j".

W poniższym przykładzie zostanie zastosowane to pierwsze rozwiązanie.

M	A	C	I	E
J	B	D	F	G
H	K	L	N	O
P	R	S	T	U
V	W	X	Y	Z

W kolejnym kroku tekst jawny dzielony jest na tzw. *digramy*, czyli pary liter. Każdy powinien składać się z dwóch różnych liter. W razie potrzeby litery powtarzające się (lub brakujące, jeśli tekst jawny nie kończy się pełnym digramem) można rozdzielić stosując jakąś jedną, umówioną literę (np. X).

Przykładowo:

Tekst jawny:	TECHNIKI OCHRONY INFORMACJI
Tekst podzielony na digramy:	TE CH NI KI OC HR ON YI NF OR MA CJ IX

Otrzymane digramy można podzielić na trzy grupy:

- obie litery znajdują się w tym samym wierszu;
- obie litery znajdują się w tej samej kolumnie;
- pozostałe.

Jeśli obie litery znajdują się w tym samym wierszu, zastępowane są sąsiadującymi z nimi literami z prawej strony – bazując na powyższym przykładzie, MA zamienia się w AC. Jeżeli jedna z liter znajduje się na samym końcu wiersza, to jest zastępowana pierwszą literą w tym wierszu.

Jeśli obie litery znajdują się w tej samej kolumnie, powinny zostać zastąpione przez litery leżące pod nimi; np. NI zmienia się w FT. Jeżeli któraś litera znajduje się na końcu kolumny, zastępowana jest pierwszą literą w kolumnie.

Jeśli natomiast każda z liter digramu znajduje się w innym wierszu i innej kolumnie, sytuacja się nieco komplikuje. W takim wypadku, aby zaszyfrować pierwszą literę, należy podążać wzdłuż wiersza, w którym się ona znajduje aż do kolumny zawierającej drugą literę. Litera na skrzyżowaniu wiersza z kolumną zastępuje pierwszą literę. W celu zaszyfrowania drugiej z liter, należy podążać wzdłuż wiersza, w którym się ona znajduje aż do kolumny, w której znajduje się pierwsza litera. Znak ze skrzyżowania reprezentuje drugą literę. Odnosząc się do powyższego przykładu, digram TE po zaszyfrowaniu przyjmie postać IU.

Tekst podzielony na digramy:	TE CH NI KI OC HR ON YI NF OR MA CJ IX
Szyfrogram:	IU LM FT NA LE KP HK IF TN KU AC DM CY

Adresat znając słowo-klucz może odczytać wiadomość odwracając opisaną procedurę. Szyfr można jednak złamać, m.in. odszukując najczęściej występujące w danym języku digramy (Schneier, 2002).

Szyfr Playfair był stosowany przez Brytyjczyków w trakcie drugiej wojny burskiej (1899-1902) oraz w trakcie I wojny światowej jako stosunkowo szybka i relatywnie bezpieczna metoda szyfrowania ważnych, lecz nie krytycznych informacji taktycznych – zanim przeciwnik zdążył odszyfrować wiadomość, jej treść stawała się już mało istotna (np. ze względu na zmiany na froncie) (Kahn, 1997).

W podobnym celu szyfr Playfair był wykorzystywany przez Niemców w czasie II wojny światowej, choć w nieco zmodyfikowanej formie – tzw. podwójnego szyfru Playfair, który wykorzystywał drugi kwadrat 5x5 składający się z drugich liter każdego z digramów, rozdzielonych kolejnymi literami słowa-klucza. Jednak ze względu na rozwój technik kryptoanalizy metoda ta nie zapewniała już odpowiedniego poziomu bezpieczeństwa (Smith, 1998).

Sama idea szyfru Playfair (oparcie się o tablicę 5x5) stanowi bardzo zmodyfikowaną formę tzw. **szachownicy Polibiusza**, czyli prostego szyfru monoalfabetycznego opisanego w *Dziejach* greckiego historyka Polibiusza. Polega on na zastąpieniu każdej litery tekstu jawnego parą liczba według następującego schematu (za: Polibiusz, 2005) :

	1	**2**	**3**	**4**	**5**
1	A	B	C	D	E
2	F	G	H	I/J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

Jako pierwszą cyfrę danej liczby podaje się numer wiersza, zaś jako drugą – numer kolumny. Przykład:

Tekst jawny: `M A C I E J L A S K O W S K I`

Szyfrogram: `32 11 13 24 15 24 31 11 43 25 34 52 43 25 24`

Szyfr ten, choć prosty do złamania dzięki analizie częstotliwościowej (tak jak każdy monoalfabetyczny szyfr podstawieniowy) stanowił podstawę wyjściową zarówno do szyfru Playfair, jak i do kilku innych, m.in. szyfru nihilistów, ADFGVX czy też szyfru bifid.

Szyfr nihilistów z lat 80.-tych XIX wieku stanowi konglomerat szachownicy Polibiusza, szyfru Playfair i tablicy Vigenère (Kahn, 1997). W pierwszym kroku należy stworzyć bowiem szachownicę Polibiusza wykorzystując do tego słowo-klucz.
W poniższym przykładzie będzie to słowo SERGIUSZ – po usunięciu powtarzających się liter przyjmujące postać SERGIUZ.

	1	**2**	**3**	**4**	**5**
1	S	E	R	G	I/J
2	U	Z	A	B	C
3	D	F	H	K	L
4	M	N	O	P	Q
5	T	V	W	X	Y

Przy pomocy powyższej szachownicy kodowany jest tekst jawny, np. MACIEJ LASKOWSKI.

Tekst jawny: M A C I E J L A S K O W S K I
Szyfrogram: 41 23 25 15 12 15 35 23 11 34 43 53 11 34 15

Dodatkowo, przy wykorzystaniu tej samej szachownicy szyfrowane jest drugie słowo kluczowe, np. NIHILIZM.

Tekst jawny: N I H I L I Z M
Szyfrogram: 42 15 33 15 35 15 22 41

Pełny szyfrogram uzyskuje się dodając do siebie szyfrogramy treści wiadomości i drugiego słowa kluczowego.

Wiadomość: 41 23 25 15 12 15 35 23 11 34 43 53 11 34 15
Klucz: 42 15 33 15 35 15 22 41 42 15 33 15 35 15 22
Szyfrogram 83 38 58 30 47 30 57 64 53 49 76 68 46 49 37

Zmodyfikowane formy szyfru nihilistów były wykorzystywane jeszcze w czasie II wojny światowej przez sowieckich agentów w krajach Osi (Kahn, 1997).

Kolejnym szyfrem opartym o szachownice Polibiusza jest **szyfr bifid**, opracowany około 1901 roku przez Felixa Delastelle (Kahn, 1997).
W pierwszej fazie nadawca wiadomości tworzy własną wersję tablicy Polibiusza:

	1	**2**	**3**	**4**	**5**
1	A	K	L	Q	V
2	B	I/J	M	R	W
3	C	H	N	S	X
4	D	G	O	T	Y
5	E	F	P	U	Z

W kolejnym kroku tekst jawny jest szyfrowany przy użyciu kolejnych wierszy i kolumn, z tym, że są one zapisywane pionowo.

Tekst jawny: M A C I E J L A S K O W S K I
Szyfrogram: 2 1 3 2 5 2 1 1 3 1 4 2 3 1 2
3 1 1 2 1 2 3 1 4 2 3 5 4 2 2

Następnie obydwa wiersze łączy się, dzieli na pary, które następnie konwertowane są na litery przy użyciu tej samej wersji tablicy Polibiusza. Odszyfrowanie tekstu polega na wykonaniu tych samych czynności w odwrotnej kolejności.

Szyfrogram: 213252113142312311212314235422
Podział na pary: 21 32 52 11 31 42 31 23 11 21 23 14 23 54 22
Postać tekstowa: B M F A C G C M A B M Q M U I

Szyfr **ADFGX** to szyfr podstawieniowy opracowany przez pułkownika Fritza Nebela w marcu 1918, używany przez wojska niemieckie w czasie I wojny światowej do komunikacji na polu bitwy.

W czerwcu 1918 opracowaną nową wersję szyfru, nazwaną **ADFGVX**, która umożliwiała nie tylko szyfrowanie liter, ale także i cyfr (Kahn, 1997).

ADFGVX jest oparty na zmodyfikowanej szachownicy Polibiusza. W wyniku zaszyfrowania tekstu jawnego otrzymuje się szyfrogram składający się z digramów liter A, D, F, G, V oraz X.

Zostały one wybrane, ponieważ różnią się znacząco od siebie podczas nadawania za pomocą alfabetu Morse'a, co umożliwiło zmniejszenie ryzyka powstania błędów przy nadawaniu lub odbiorze wiadomości (Kahn, 1997).

Przykład działania:

	A	**D**	**F**	**G**	**V**	**X**
A	A	L	M	X	Y	5
D	B	K	N	W	Z	6
F	C	J	O	V	1	7
G	D	I	P	U	2	8
V	E	H	Q	T	3	9
X	F	G	R	S	4	0

Tekst jawny: M A C I E J L A S K O W S K I

Szyfrogram: AF AA FA GD VA FD AD AA XG DD FF DG XG DD GD

W kolejnym kroku wprowadzane było słowo-klucz, któremu przypisywano poszczególne litery kodu według następującego schematu (dla słowa SERGIU):

Słowo-klucz: S E R G I U

Szyfrogram: A F A A F A

G D V A F D

A D A A X G

D D F F D G

X G D D G D

W kolejnym kroku kolumny są sortowane alfabetycznie według liter słowa-klucza.

Słowo-klucz:	E	G	I	R	S	U
Szyfrogram:	F	A	F	A	A	A
	D	A	F	V	G	D
	D	A	X	A	A	G
	D	F	D	F	D	G
	G	D	G	D	X	D

Szyfrogram jest następnie odczytywany kolumnowo.

FA FA AA DA FV GD DA XA AG DF DF DG GD GD XD

Zarówno układ liter w zmodyfikowanej szachownicy Polibiusza, jak i słowa-klucze były zmieniane codziennie.

Niemcy do końca I wojny światowej uważali ten szyfr za niemożliwy do złamania. Jednak zarówno ADFGX, jak i ADFGVX zostały złamane w przeciągu miesiąca od ich wdrożenia przez francuskiego kryptoanalityka Georgesa Painvina, który m.in. wykorzystał fakt, iż pewne stereotypowe nagłówki wiadomości formowały identyczne wzorce w szyfrogramie, odnoszące się do nagłówków kolumn w macierzy ze słowem-kluczem (Childs, 2000). Kryptoanaliza tą metodą była możliwa jednak tylko w okresach, kiedy przesyłano dużą ilość wiadomości, jak np. przed rozpoczęciem ofensywy (Childs, 2000). Odszyfrowanie jednej wiadomości pozwalało na odczytanie wszystkich wiadomości zaszyfrowanych przy użyciu tej samej tablicy oraz słowa-klucza (Kahn, 1997).

2.3 Szyfry Agencji Wschodniej

Agencja Wschodnia to niesłusznie zapomniana polska placówka dyplomatyczna, działająca w XIX wieku. Jej centrala mieściła się w Stambule, ale jawni współpracownicy i zakamuflowani agenci przemierzali całą Europę Wschodnią począwszy od Bałkanów, Ukrainy, Rumunii aż po Kaukaz Północny, Zakaukazie i wschodnie rubieże Turcji (Łątka, 1985).

Agencja została powołana do życia przez księcia Adama Jerzego Czartoryskiego (Fot. 2.10), stojący na czele Hotelu Lambert, który stanowił w owym czasie, jeśli nie namiastkę rządu polskiego na uchodźstwie, to na pewno był najistotniejszym ośrodkiem politycznym realizującym interesy nieistniejącej wówczas Polski na świecie. Najważniejszym było oczywiście odzyskanie niepodległości (Łątka, 1985).

Fot. 2.10 Książę Adam Jerzy Czartoryski
(źródło: Nadar, 2012)

Po klęsce powstania listopadowego książę Czartoryski rozpoczął zakulisowe działania mające na celu wciągnięcie Rosji w jak największą liczbę konfliktów zbrojnych, co starał się osiągnąć wspomagając lokalne ruchy narodowo-wyzwoleńcze w krajach Europy Centralnej, Wschodniej oraz Kaukazu (Łątka, 1985).

W 1841 roku uznał, że dla interesów Polski ważne jest posiadanie przyczółku maksymalnie zbliżonego do Rosji.

Utworzenie centrali Agencji Wschodniej w Stambule było możliwe między innymi dzięki przychylnej postawie Turcji, która jako jedno z niewielu państw nie uzna-wała rozbiorów Polski i według niektórych źródeł na międzynarodowych spotkaniach politycznych w rządzie tureckim pozostawiano zawsze jedno miejsce wolne „dla posła Lechistanu, który nie mógł przybyć z przyczyn obiektywnych".

Jednak niezależnie od sympatii dla Polski, Turcja pozostawała w ścisłych związkach gospodarczych i politycznych z Rosją. Aktywność dyplomatyczna i szpiegowska wymagała więc wielkiej ostrożności i wykorzystania odpowiednich środków ochrony informacji. O skali polskiego przedsięwzięcia może świadczyć fakt, że agenci Czartoryskiego pojawiali się w Grecji, Bułgarii, Serbii i Rumunii (Łątka, 1985).

Spektrum technik kryptograficznych stosowanych przez Agencję było jak na XIX wiek całkiem szerokie – agenci polscy w codziennej korespondencji stosowali co najmniej kilka rodzajów szyfrów i kodów, a także techniki steganograficzne, takie jak chociażby atrament sympatyczny.

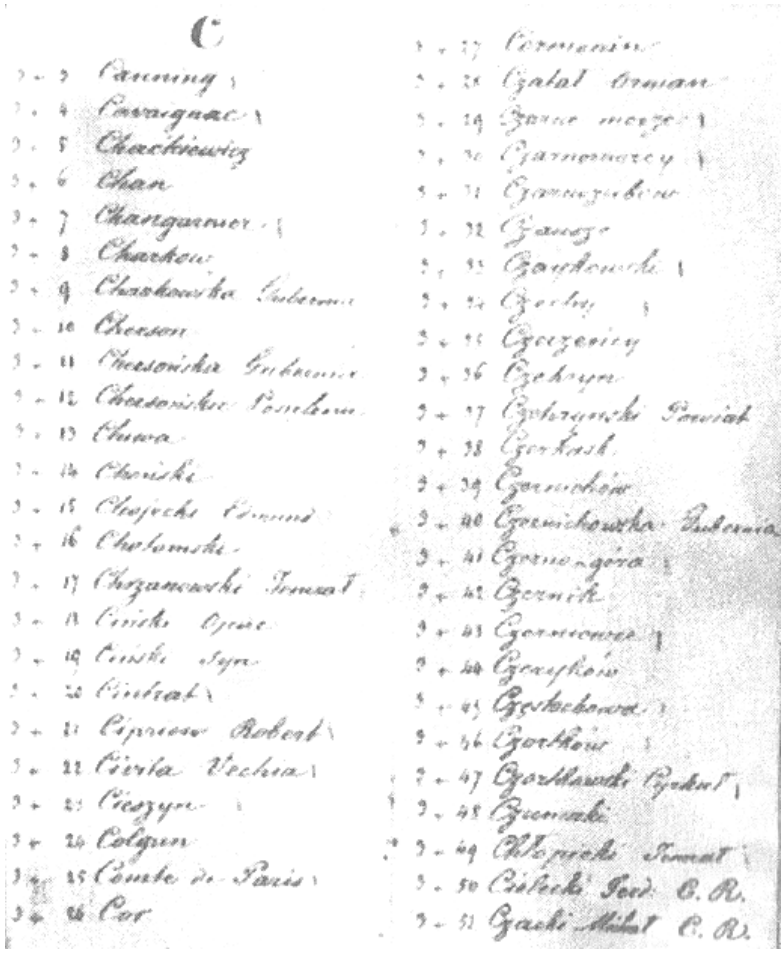
Pierwszym rodzajem kodu używanym do ochrony nazwisk kluczowych kontaktów lub istotnych miejsc, o których pisano w korespondencji była klasyczna książka kodowa – czyli de facto nomenklator. Każdemu słowu, które chciano ukryć przypisywano odpowiedni symbol alfanumeryczny. Agent posługiwał się nim konsekwentnie w całej korespondencji (Łątka, 1985).

Fragment raportu z kwietnia 1850 roku (za: Łątka, 1985):

Przybycie (2, 6+32) nie może być policzonem za pomyślny wypadek dla nas. Jak sam (3+26) powiada siła i wszem mocność (3, 12+24) zanadto silne wywarły na nim wrażenie, a już mniemam, że pozobowiązywał się (313+22) wbrew przeciwnym postanowieniom (2, 4+52).

W cytowanym raporcie każda sekwencja cyfr umieszczona w nawiasach oznaczała określone nazwisko lub nazwę, najczęściej były to nazwiska osób, tajnych współpracowników lub dyplomatów, z którymi kontaktowali się agenci.

Na podstawie fragmentu księgi kodowej, przedstawionego na Fot. 2.11, sekwencja 3+26 oznacza „Cor", co było nazwiskiem Francuza zatrudnionego w konsulacie francuskim w Stambule, 6+32 – tureckiego dyplomatę Fuada, 313+32 – księcia Karla Roberta Nesselrode, ówczesnego ministra spraw zagranicznych Rosji, 12+24 oznaczało Rosję, zaś 4+52 – turecką Radę Państwa.



Fot. 2.11. Fragment księgi kodowej
(źródło: Łątka, 1985)

Pracownicy Agencji musieli mieć pewną wiedzę na temat postępów kryptoanalizy w owym czasie – skutecznym sposobem na rozszyfrowanie przynajmniej części kodów byłaby analiza sekwencyjna, które występują najczęściej i obserwowanie, w jakich kontekstach się one pojawiają oraz jakie rzeczywiste zdarzenia im odpowiadają. Zabezpieczeniem przez analizą statystyczną miało być stosowanie homofonów. Przykładem może być Michał Czaykowski, szef Agencji, który pojawiał się praktycznie w każdym liście wysyłanym przez agentów – na oznaczenie jego osoby stosowano co najmniej kilkanaście oznaczeń, m.in. (MCD), (XIII), (14), (93+29), (IV), (IX) , (VII), (Aa), (AGH+) i wiele innych (Łątka, 1985).

Inna książka kodowa stosowana przez Agencję była oparta o kompletny słownik języka polskiego, w którym każdemu słowu przypisano jeden kod składający się z liter i znaków przestankowych.

Fragment książki kodowej (za: Łątka, 1985):

z + a – abdykacja
z + b – abdykować
z + c – abecadło
z + d – abiuracja

Ze względu na skomplikowane formy fleksyjne języka polskiego stosowano również dodatkowe mechanizmy ich zapisu w oparciu o słowo bazowe. Cyfra dodawana w nawiasie przed kodem pozwalała zasygnalizować zmianę przypadku, a plus dodany po kodzie – liczbę mnogą. I tak (y mn) oznaczało „buntownik", (y mn+) – „buntownicy", zaś (3, y mn+) – „buntownikom" (Łątka, 1985).

Dodatkowo za pomocą cyfr umieszonych w górnym lub dolnym indeksie kodów sygnalizowano zmianę czasu (dla czasowników), rodzaju osobowego (dla przymiotników), imiesłowy czy też stopniowanie.

Przykładowo (w+hh) oznaczało „dobry", zaś (w+hh^{2}_{1}) – „najlepsza" (Łątka, 1985).

Systemy stosowane przez agentów udających się w samodzielne misje, nieraz bardzo oddalone od centrali, musiały dodatkowo spełniać warunek łatwości stosowania. Ograniczano w związku z tym liczbę kodów oraz możliwych kombinacji, uzyskując kod prostszy w użyciu kosztem precyzji języka. Wykorzystywano tutaj

np. książkę kodową opartą o imiona, których modyfikacje pozwalały przekazywać podstawowe formy fleksyjne. Słowo „Eugenius" w formie podstawowej oznaczało „Polskę", bez ostatniej litery („Eugeniu") – „Warszawę", a „Eugeniuss" – „Polaków" (Łątka, 1985).

Jednym z najciekawszych szyfrów stosowanych przez Agencję jest szyfr homofoniczny oparty o „tajny alfabet" z dodatkowym graficznym mechanizmem generowania klucza. Szyfr był dwuetapowy i oparty o spersonalizowany klucz kryptograficzny, generowany w oparciu o hasło znane tylko jego posiadaczowi.

Kluczem osobistym mogło być nazwisko lub sentencja, która nie powinna być nigdzie zapisana – poza tymczasowym arkuszem stosowanym przy szyfrowaniu i odszyfrowaniu wiadomości. Słowo było zapisywane w tabelce o trzech grupach po trzy kolumny. Grupy trzech kolumn były rozdzielone pionowymi kreskami, poziome kreski rozdzielały każdy wiersz, co było istotne przy późniejszej reprezentacji graficznej klucza (Łątka, 1985).

Generowanie klucza odbywa się w sposób zbliżony do techniki szyfru Vigenère – na początku sekwencji wpisuje się hasło, pomijając powtarzające się litery, a za nim kolejne litery alfabetu, pomijając te, które były już użyte.
Przykładowo, w tabeli przydzielonej agentowi Władysławowi Chrzanowskiemu, słowem-kluczem było jego nazwisko (za: Łątka, 1985):

1	2	3	1	2	3	1	2	3
C	H	R	Z	A`	N	O	W	S
K	I	B	D	E	F	G	J	L
M	P	Q	T	U	X	Y		

Szyfrowanie przy pomocy takiej tabeli polegało na wyszukaniu znaku tekstu jawnego w tabeli, a następnie podaniu cyfry oznaczającej kolumnę, w której on występował. Ponieważ dana cyfra mogła oznaczać literę w jednej z trzech grup, konieczne było podanie wiersza. Cyfrę umieszczano więc dodatkowo w graficznym symbolu wskazującym na jej położenie w tabeli.

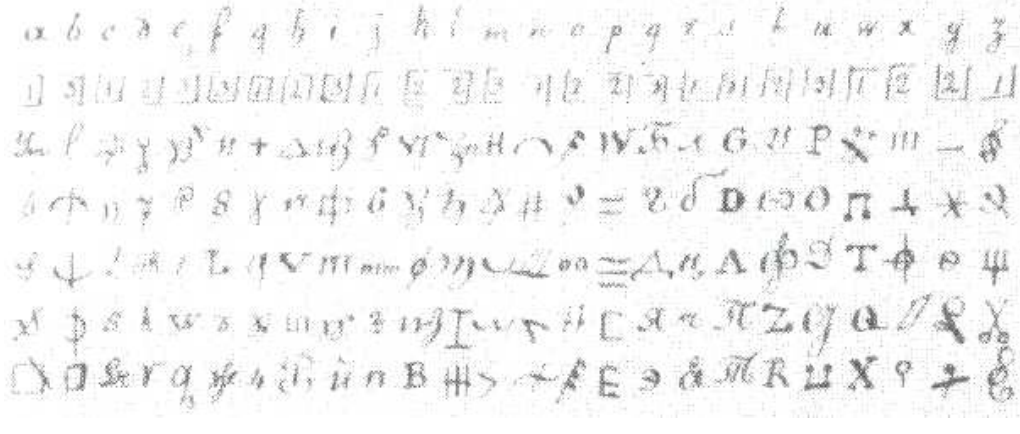
Słowo „POLSKA” zaszyfrowane kluczem Władysława Chrzanowskiego wyglądałoby następująco:

2	1	3	3	1	2
P	0	L	S	K	A

Zasada działania szyfru zostanie omówiona na przykładzie litery P.
Jej reprezentacją graficzną jest

Powyższy zapis oznacza, że właściwa litera znajduje się w drugiej kolumnie grupy wskazywanej przez symbol graficzny – ponieważ taki układ linii występuje tylko w prawym, dolnym narożniku tabeli, pozwala to jednoznacznie określić, że chodzi o literę P.

System ten łączył stosunkową łatwość stosowania ze względnym bezpieczeństwem, ponieważ każdy użytkownik stosował swój indywidualny klucz szyfrujący. W podstawowej postaci system jest jednak podatny na analizę częstotliwościową, przed którą ochronę miał zapewniać drugi element systemu jakim była tablica homofoniczna – każdy znak mógł być szyfrowany na wiele symboli wyjściowych (vide Fot. 2.12).



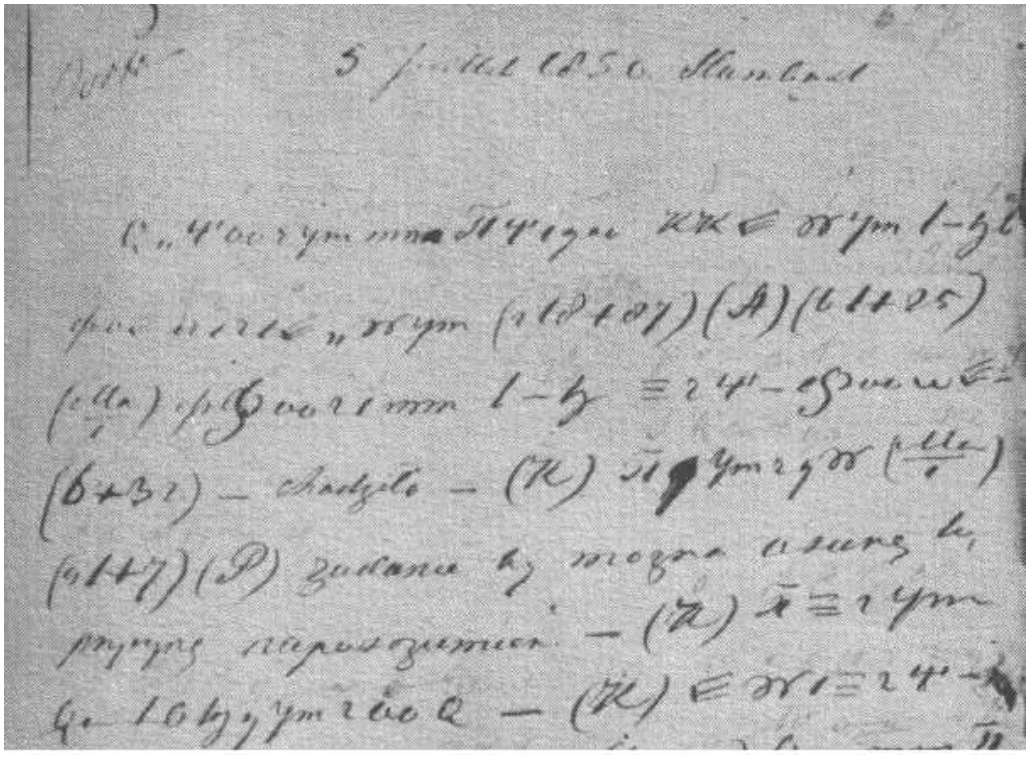
Fot. 2.12. Tablica homofoniczna używana przez agentów Misji Wschodniej (źródło: Łątka, 1985)

Pierwsze dwa wiersze zawierają podstawienia wygenerowane przy pomocy opisanej powyżej tabelki, podczas gdy kolejne wiersze zawierają symbole homofoniczne – agent miał obowiązek ich używania w przypadku, jeśli dany znak powtarzał się w tekście więcej niż raz.

Zatem do zaszyfrowania litery „H" za pierwszym razem użyto by symbolu z tabeli, za drugim razem znaku trójkąta itd.

Fragment rzeczywistej korespondencji z 1850 roku wykorzystującej wszystkie zaprezentowane techniki został zaprezentowany na fotografii 2.13.

Autor zastosował zarówno symbole z książki kodowej na oznaczenie znanych nazwisk lub miejsc, jak i opisany wyżej szyfr homofoniczny do utajnienia nazw i słów, które prawdopodobnie nie miały przypisanych własnych kodów.



Fot. 2.13. Fragment korespondencji wykorzystującej opisywaną metodę szyfrowania (źródło: Łątka, 1985)

2.4 ENIGMA

Pomimo, iż Enigma nie była pierwszym urządzeniem szyfrującym – wystarczy wspomnieć opisany powyżej Dysk Jeffersona czy opracowaną w 1929 maszynę Hilla (Overbey, Traves & Wojdylo, 2005) – to jednak właśnie ona stała się najpopularniejszą ilustracją idei maszyn wspierających proces szyfrowania informacji. Stało się tak głównie ze względu na skomplikowaną historię łamania kodów rozgrywającą się przed i w trakcie II wojny światowej. Ze względu na znacznie dla historii kryptografii i kryptologii, a także na znaczący wkład Polaków w złamanie tajemnic Enigmy, warto się tej historii przyjrzeć nieco dokładniej.

2.4.1 POWSTANIE ENIGMY

W roku 1918 niemiecki inżynier Arthur Scherbius złożył wniosek patentowy na wirnikową maszynę szyfrującą, którą nazwano później Enigma (z gr. zagadka) (Kahn, 1997). Planowanymi użytkownikami tej maszyny miały być głownie wielkie firmy chcące chronić swoją korespondencję, a także inne instytucje państwowe. Początkowo armia niemiecka nie wykazała zainteresowana wprowadzeniem maszyn szyfrujących na miejsce powszechnego w tym czasie kodu ręcznego. Jednak plany remilitaryzacyjne Republiki Weimarskiej oraz odkrycie faktu, iż służby Królestwa Brytyjskiego regularnie czytały depesze niemieckie w czasie I wojny światowej, spowodowały, że dowództwo niemieckie zdecydowało się na wprowadzenie kodu maszynowego, stanowiącego gwarancję zachowania bezpieczeństwa przekazywania informacji (Kahn, 1997).

Pierwszy model cywilny – Enigma A – był dość duży i ciężki, głównie ze względu na zintegrowaną maszynę do pisania. Dopiero Enigma C (1926) została wyposażona w walec odwracający – kluczowy element w konstrukcji maszyn Enigma (Kahn, Enigma. Złamanie kodu U-Bootów 1939-43, 2005).

Wersja C była mniejsza i nadawała się do przenoszenia – zrezygnowano w niej bowiem ze zintegrowanej maszyny do pisania, wprowadzając w zamian panel z literami podświetlanymi żarówkami (Kahn, Enigma. Złamanie kodu U-Bootów 1939-43, 2005). Enigma C była używana dość krótko, gdyż już w 1927 roku zastąpiono ją

maszyną Enigma D, która poza Niemcami była wykorzystywana również w Szwecji, Holandii, Anglii, Japonii, Włoszech, Hiszpanii, Stanach Zjednoczonych i Polsce. Cywilną odmianę Enigmy można było bez utrudnień nabyć na rynku. Prawdopodobnie armia niemiecka celowo nie dążyła do wycofania maszyny z rynku, aby nie zwrócić uwagi służb specjalnych innych krajów jej nagłym zniknięciem (Piekałkiewicz, 1999).

W roku 1926 przyjęto Enigmę na wyposażenie niemieckiej marynarki wojennej jako Funkschlüssel C (Koder radiowy C). Zaowocowało to szybkim rozwojem wojskowych wersji urządzenia. Klawiatura maszyny i panel z lampkami zawierały 29 liter – A-Z, Ä, Ö i Ü – które były umieszczone alfabetycznie, a nie tak jak na standardowej klawiaturze niemieckiej QWERTZ (Kozaczuk, 1984).

Od 1928 niemiecka Reichswehra wprowadziła do służby własną wersję Enigmy oznaczoną jako Enigma G, która w lipcu 1930 została zmodyfikowana do wersji Enigma I, która była intensywnie używana także przez inne niemieckie organizacje wojskowe i rządowe (takie jak kolej niemiecka), zarówno przed jak i w czasie II wojny światowej. Główną różnicą między handlową wersją Enigmy i Enigmą I było dodanie łącznicy kablowej do zamiany liter parami, co zwiększało bezpieczeństwo szyfru maszyny (Nowik, 2004). Inną różnicą było zastosowanie nieruchomego walca odwracającego i przeniesienie wcięć zębatki obracającej wirniki z obudowy wirnika na pierścień alfabetyczny (vide Rozdział 2.3.2).

W 1930 zasugerowano Kriegsmarine zaadaptowanie Enigmy do własnych potrzeb, prezentując zwiększone bezpieczeństwo wersji z łącznicą kablową oraz łatwiejszą łączność między różnymi rodzajami sił zbrojnych. Ostatecznie Kriegsmarine przyjęła Enigmę na wyposażenie w 1934 wybierając zmodyfikowaną wersję używaną przez siły lądowe oznaczoną Funkschlüssel M lub M3. Wojska lądowe i Luftwaffe wykorzystywały w tym czasie zestaw trzech typów wirników, ale Kriegsmarine dla zwiększenia bezpieczeństwa zamówiła zestaw 5 typów wirników, z których do zainstalowania można było wybrać trzy z nich (Kozaczuk, 1984).

W grudniu 1938 także inne formacje Wehrmachtu zaczęły wykorzystywać rozszerzony do pięciu typów zestaw wirników. W 1938 Kriegsmarine wzbogaciła swój zestaw wirników o dodatkowe dwa typy i kolejny typ w 1939, co ostatecznie dało zestaw ośmiu typów wirników (Kozaczuk, 1984). W sierpniu 1935 również Luftwaffe

zaczęła stosować do komunikacji maszyny Enigma w wersji używanej przez siły lądowe (Kozaczuk, 1984).

Pierwsza czterowirnikowa Enigma została wprowadzona po raz pierwszy w Kriegsmarine w 1942 z przeznaczeniem do łączności z niemieckimi okrętami podwodnymi. Dodatkowy, znacznie cieńszy wirnik został umieszczony w maszynie wraz z nowym, również cieńszym, walcem odwracającym (Kozaczuk, 1984).

Abwehra wykorzystywała maszynę w wersji Enigma G. Ta wersja Enigmy posiadała cztery wirniki z wieloma wcięciami, które powodowały częstsze obroty podczas szyfrowania, ale nie posiadała przełącznicy kablowej (Kozaczuk, 1984). Dodatkowo maszyna posiadała licznik, którego stan zwiększał się po każdym naciśnięciu klawisza, przez co zyskała dodatkową nazwę *Zahlwerk Enigma* (niem. licznik).

Poza Niemcami Enigmę wykorzystywano także w innych krajach. Marynarka wojenna Włoch zaadaptowała do celów wojskowych handlową wersję maszyny nazwaną jako *Koder Marynarki D* (Piekałkiewicz, 1999).

Hiszpania wykorzystywała Enigmy podczas wojny domowej, zaś w szwajcarskiej armii i dyplomacji korzystano z maszyn Enigma oznaczonych jako model K lub Swiss K, które były bardzo podobne do handlowej wersji cywilnej Enigma D (Piekałkiewicz, 1999). Ta wersja maszyny została rozszyfrowana przez wiele zespołów kryptologów z Polski, Francji, Wielkiej Brytanii i Stanów Zjednoczonych (ostatnia nazwa kodowa to INDIGO).

Enigma T oznaczona nazwą kodową *Tirpitz* została wyprodukowana specjalnie dla Japonii (Piekałkiewicz, 1999).

2.4.2 Budowa Enigmy

Enigma jest połączeniem systemów elektrycznego i mechanicznego. Część mechaniczna składa się z alfabetycznej dwudziestosześcioznakowej klawiatury, zestawu osadzonych na wspólnej osi i obracających się bębenków nazywanych rotorami lub wirnikami (niem. *Chiffrierwalzen*) oraz mechanizmu obracającego jeden lub kilka rotorów naraz za każdym naciśnięciem klawisza (Kozaczuk, 1984).

Części mechaniczne służą jako elementy obwodu elektrycznego – właściwe kodowanie liter odbywa się elektrycznie. Po naciśnięciu klawisza obwód elektryczny

zamyka się, zaś prąd przepływa przez elementy składowe maszyny, powodując zapalenie się jednej z lampek podświetlających literę wyjściową (Kozaczuk, 1984).

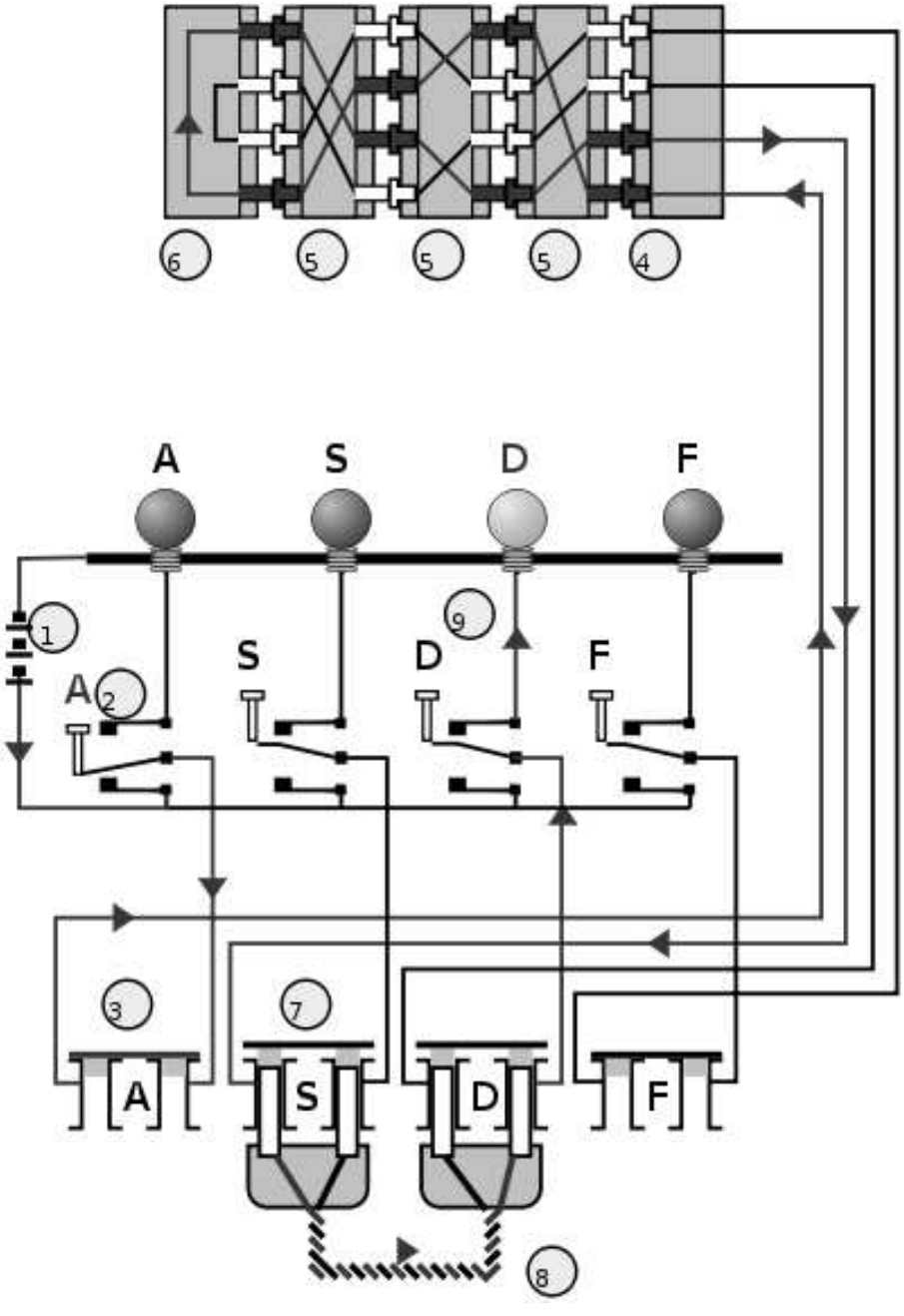
Na przykład, jeśli kodowana wiadomość zaczyna się od liter ALA, operator naciska najpierw literę „A", która może spowodować zapalenie się lampki z literą „Z". W ten sposób pierwszą literą zakodowanej wiadomości będzie „Z". Następnie operator naciska klawisz z literą „L", która zostaje analogicznie zakodowana i tak dalej.

Wyjaśnienie działania Enigmy pokazano na rysunku 2.14. Dla uproszczenia przykładu pokazane zostały tylko cztery zestawy kodujące, lampki, klawisze, kable łącznicy, podczas gdy w rzeczywistości było ich aż 26.

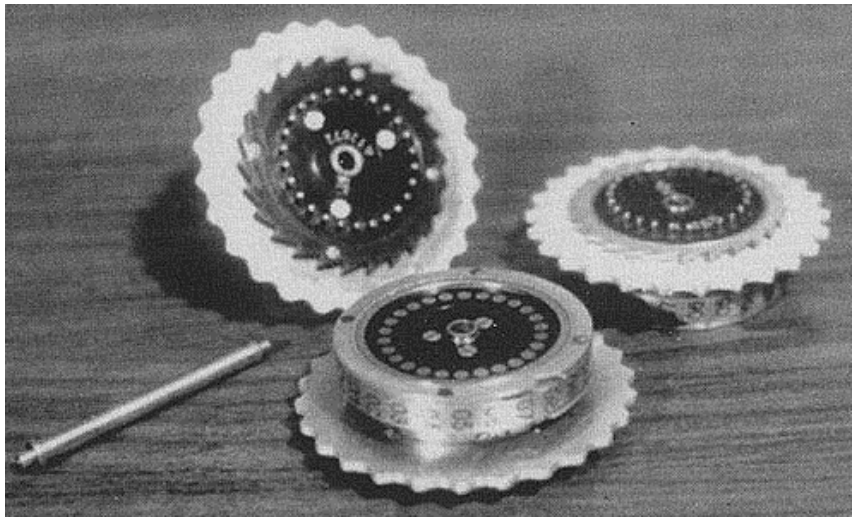
Prąd przepływa z baterii (1) przez obwód posiadającego dwa styki klawisza z literą (2) do łącznicy kablowej (3). Łącznica umożliwiała zamianę dwóch liter miejscami, jednocześnie zapewniała połączenie klawiatury (2) z walcem wstępnym (4). Prąd przepływa przez łącznicę kablową (3) do walca wstępnego (4), a następnie przez trzy (model stosowany przez niemieckie wojska lądowe) lub cztery (model stosowany przez Kriegsmarine) wirniki do bębenka odwracającego (6).
Bęben odwracający zawraca sygnał z powrotem przez wirniki (5), ale inną drogą do walca wstępnego (4) następnie doprowadzając go do gniazda 'S' łącznicy, a stamtąd przewodem do gniazda 'D' i dwustykowego klawisza (9), powodując zaświecenie się lampki.

Wirniki (przedstawione na fotografii 2.15) stanowiły serce Enigmy – ich ciągłe obracanie się powodowało bezustanne zmienianie drogi sygnału i kodowanie wiadomości szyfrem polialfabetycznym, który na ówczesne czasy zapewniał bardzo wysokie bezpieczeństwo transmisji.

Wirniki miały postać kół wykonanych z twardej gumy lub bakelitu z mosiężnymi pinami na sprężynkach z jednej strony i płaskimi stykami elektrycznymi ułożonymi w kształt okręgu z drugiej.



Rys. 2.14. Schemat okablowania Enigmy wskazujący przepływ prądu podczas naciskania litery 'A', która kodowana jest jako 'D' (źródło: Wikimedia Commons)



Fot. 2.15. Trzy wirniki Enigmy i oś, na której się je osadza.
(źródło: ed-thelen.org, 2012)

Ułożenie pinów i styków jest takie samo jak opis literowy na pierścieniu alfabetycznym wirnika – typowo były to litery od A do Z. Gdy wirniki są ułożone jeden za drugim na wspólnej osi, piny jednego z nich stykają się z płaskimi stykami elektrycznymi sąsiedniego, zamykając obwód elektryczny. Wewnątrz wirnika znajdowało się 26 przewodów łączących (zgodnie z założoną kombinacją) piny z jednej ze stykami po drugiej stronie.

Sposób okablowania był inny dla każdego typu wirnika.

Pojedynczy wirnik zapewnia tylko proste szyfrowanie szyfrem podstawieniowym (Kozaczuk, 1984). Przykładowo pin odpowiadający literze E może być połączony ze stykiem od litery T po drugiej stronie. Złożoność systemu szyfrowania polega na zastosowaniu wielu równoległych współosiowych wirników – przeważnie trzech lub czterech – oraz regularnego obracania ich, co zapewnia jeszcze większy stopień komplikacji szyfrowania (Kozaczuk, 1984).

Po włożeniu do maszyny szyfrującej, wirnik mógł być ustawiony w jednej z 26 pozycji (Kozaczuk, 1984). Przekręcenie bębenka umożliwiał przytwierdzony do niego karbowany pierścień wystający przez górną pokrywę maszyny po jej zamknięciu (Kozaczuk, 1984).

Aby operator maszyny mógł ustawić wirnik w odpowiedniej pozycji przymocowano do niego pierścień alfabetyczny z 26 literami lub cyframi, z których właściwa odpowiadająca nastawieniu pozycji była widoczna w specjalnym okienku pokrywy maszyny. We wczesnych modelach maszyny pierścień alfabetyczny był zamocowany do wirnika, ale później, w celu zwiększenia komplikacji szyfru, wprowadzono wirniki o zmiennym ustawieniu pierścienia alfabetycznego (Kozaczuk, 1984).

Modele Enigmy stosowane w wojskach lądowych i Luftwaffe były wyposażone w kilka typów wirników – początkowo tylko trzy, jednak w 1938 zwiększono zestaw wirników do pięciu, z których do zamontowania w maszynie wybierano trzy (Kozaczuk, 1984). Dla odróżnienia bębenki były oznaczane rzymskimi cyframi I, II, III, IV i V. Każdy z nich miał jedno zlokalizowane w różnych miejscach pierścienia alfabetycznego wcięcie służące do obracania go, przez co złożoność szyfru znacznie wzrastała (Kozaczuk, 1984).

Enigmy używane przez Kriegsmarine były wyposażone w większy zestaw wirników. Początkowo było ich sześć, później siedem, by ostatecznie osiągnąć liczbę ośmiu (Kozaczuk, 1984). Dodatkowe wirniki oznaczone jako VI, VII i VIII były okablowane w różny sposób i posiadały po dwa wcięcia na wysokości liter „N” i „A”, które umożliwiały ich częstsze obracanie (Kozaczuk, 1984).

Enigma M4 posiadała czwarty wirnik, którego zastosowanie nie wymagało przebudowy samej standardowo trójwirnikowej maszyny (Kozaczuk, 1984). Dodatkowe miejsce uzyskano poprzez zastosowanie nowego cieńszego bębenka odwracającego i specjalnego czwartego wirnika, który nigdy się nie obracał, ale mógł być ustawiony ręcznie w jednej z dwudziestu sześciu pozycji. Czwarty wirnik był produkowany w dwóch wersjach oznaczonych jako Beta i Gamma (Kozaczuk, 1984).

W celu zwiększenia komplikacji kodu niektóre wirniki poruszały się nie za każdym naciśnięciem klawisza. Takie działanie zapewnia odmienne kodowanie znaku w każdej pozycji bębenków i powstanie w efekcie bardzo skomplikowanego polialfabetycznego szyfru podstawieniowego (Kozaczuk, 1984).

Obracanie wirników zrealizowano za pomocą mechanizmu zębatkowo-zapadkowego. Na każdy z wirników maszyny nałożone zostały koła zębate o 26 zębach współpracujących z zapadkami.

Każde naciśnięcie klawisza maszyny powoduje jednoczesne popchnięcie zapadek, które, jeśli natrafią na występ zębatki bębenka, powodują jego obrót.

W Enigmie używanej przez siły lądowe i powietrzne na wirniki założono dodatkowe koło z wcięciem (Kozaczuk, 1984). Pięć podstawowych wirników (I-V) miało po jednym wcięciu, natomiast dodatkowe wirniki maszyn Kriegsmarine (VI-VIII) po dwa (Kozaczuk, 1984).

W pewnych pozycjach wcięcie to ustawiało się w takiej pozycji, że zapadka sąsiedniego wirnika umożliwiała przestawienie dwóch bębenków jednocześnie (Kozaczuk, 1984). W przeciwnym razie zapadka ślizga się po powierzchni koła z nacięciem nie powodując dodatkowego obrotu (Kozaczuk, 1984). Dla wirników mających jedno wcięcie dodatkowy skok drugiego bębenka następuje co 26 obrotów pierwszego bębenka i podobnie – obrót trzeciego co 26 obrotów drugiego (Kozaczuk, 1984). Drugi wirnik obraca się w taki sam sposób jak trzeci, dlatego w pewnym momencie przeskoczy on o dwa ząbki za jednym naciśnięciem klawisza skracając tym samym swój okres obrotu.

Fakt występowania tego podwójnego kroku w Enigmie, odróżnia sposób obracania się bębenków od np. samochodowego licznika kilometrów. Podwójny krok zachodzi, gdy pierwszy wirnik skokowo wykonuje obrót, a w momencie natrafienia zapadki na wcięcie w drugim wirniku następuje przestawienie go o jeden krok do przodu. Tak samo dzieje się z trzecim wirnikiem, jednak w momencie natrafienia zapadki na wcięcie zostaje on obrócony o jeden krok wraz z drugim bębenkiem. W kolejnym cyklu zapadka popycha drugi wirnik po raz kolejny (drugi raz z rzędu).
Po naciśnięciu klawisza na klawiaturze Enigmy, najpierw następuje obrót wirników, a dopiero później jest zestawiany obwód elektryczny.

Z wyjątkiem pierwszych dwóch modeli Enigmy, oznaczonych literami A i B, wszystkie późniejsze maszyny posiadały walec odwracający. Było to opatentowane rozwiązanie odróżniające Enigmę od innych ówcześnie budowanych maszyn szyfrujących z wirnikami. Zadaniem walca odwracającego było połączenie styków elektrycznych ostatniego wirnika kodującego w pary i zawrócenie sygnału inną drogą przez zestaw wirników. Z tego powodu walec odwracający nazywano także reflektorem (Kozaczuk, 1984).

Jest on symetryczny, co oznacza, że zaszyfrowana informacja jest rozkodowywana po przesłaniu jej tą sama drogą (powtórnym zakodowaniu). Bęben ten nadaje Enigmie jeszcze jedną własność, mianowicie, nigdy żadna litera przed zaszyfrowaniem nie może mieć tej samej wartości co zaszyfrowana (czyli nigdy „A" nie będzie po zaszyfrowaniu występować jako „A"). Wynika to z konstrukcji bębna, który zawsze zamienia znaki parami.
Własność ta, choć miała być zaletą, jest w rzeczywistości błędem kryptologicznym i została wykorzystana do złamania kodu Enigmy.

W wersji komercyjnej typu C walec odwracający mógł być zainstalowany w jednej z dwóch pozycji, natomiast w nowszej wersji D w jednej z 26 pozycji, ale nie poruszał się on podczas szyfrowania. W wersji Enigmy przeznaczonej dla Abwehry walec odwracający obracał się tak samo jak pozostałe wirniki. Urządzenia wykorzystywane przez wojska lądowe i Luftwaffe również posiadały nieruchome bębenki odwracające, które produkowano w czterech wersjach (Large, 2003).

Kolejnym istotnym elementem była łącznica kablowa, która umożliwia różnorodne okablowanie, które może być zmieniane przez operatora (Large, 2003). Mimo swej prostoty pozwalała na znaczny wzrost komplikacji szyfru, większy niż dodatkowy wirnik (Large, 2003). Enigma bez łącznicy mogła być rozkodowana w relatywnie prosty sposób nawet metodami ręcznymi, natomiast zamiana liter przy pomocy łącznicy kablowej wymusiła zastosowanie do łamania kodów specjalnych maszyn (Large, 2003).

Przewody łącznicy kablowej pozwalały zamienić niektóre pary liter miejscami, np. „E" i „Q" (Large, 2003). Efektem była zamiana liter zarówno przed jak i po przejściu sygnału przez wirniki kodujące. Przykładowo po naciśnięciu przez operatora klawisza E sygnał jest kierowany do Q a następnie wprowadzany na wirniki. W tym samym czasie można zamienić do 13 par liter (cały dwudziestosześcioznakowy alfabet).

Odbywa się to w następujący sposób: sygnał elektryczny biegnie z klawiatury przez łącznicę kablową do walca wstępnego. Każda litera na łącznicy posiada dwa gniazda, w które wkłada się wtyczkę. Po włożeniu wtyczek następuje odłączenie górnych wtyków od klawiatury i dolnych od walca wstępnego maszyny. Sygnał elektryczny przebiega kablem zamieniając połączenia dwóch liter miejscami.

Dodatkowo, Enigma wyposażona była w różnego rodzaju dodatkowe akcesoria, które miały wspomóc pracę osoby obsługującą ją. Jednym z popularniejszych urządzeń był Schreibmax – drukarka mogąca drukować cały zestaw 26 znaków na wąskiej papierowej taśmie (Garliński, 1999). Dzięki temu Enigmę mógł obsługiwać tylko jeden operator – zadaniem drugiego operatora było odczytywanie sygnałów z lampek i zapisywanie odkodowanej wiadomości. Schreibmax był instalowany na górnej pokrywie maszyny i podłączany zamiast panelu z lampkami, który na czas używania drukarki demontowano. Poza oczywistą wygodą użytkowania zastosowanie Schreibmaxa zwiększyło również bezpieczeństwo transmisji, gdyż możliwe było zdalne zainstalowanie drukarki, choćby w drugim pomieszczeniu, co uniemożliwiało wprowadzającemu szyfrogram operatorowi odczytanie zdekodowanej wiadomości.
Zamiast drukarki wykorzystywano tez często zdalny panel z lampkami, umożliwiający odczyt wiadomości w drugim pomieszczeniu lub poza zasięgiem wzroku operatora (Garliński, 1999).

2.4.3 ENIGMA – SPOSÓB UŻYCIA

Niemiecka komunikacja wojskowa została podzielona na wiele różnych sieci, z których każda używała innych ustawień dla używanych w niej maszyn.
Każda z jednostek działających w danej sieci otrzymywała co pewien czas listy ustawień Enigmy. W celu prawidłowego przesłania wiadomości obydwie maszyny – zarówno nadawcza, jak i odbiorcza – musiały być identycznie ustawione, włączając w to ten sam zestaw wirników ustawionych w takich samych pozycjach startowych i z identycznie okablowaną łącznicą kablową (Kozaczuk, 1984).

Wszystkie dane o ustawieniach maszyn ustalano z wyprzedzeniem i drukowano w postaci książek kodowych. Warto zauważyć, że dla samych książek kodowych także opracowano odpowiednie procedury zabezpieczające: przykładowo te używane przez Kriegsmarine były drukowane przy użyciu czerwonego, rozpuszczalnego w wodzie tuszu na różowym papierze, co miało zapewnić łatwość jej zniszczenia w przypadku niebezpieczeństwa przejęcia jej przez nieprzyjaciela (Kozaczuk, 1984).

Klucz Enigmy zawierał następujące dane (za: Kozaczuk, 1984):

- kolejność wirników – zestaw typów wirników oraz kolejność, w jakiej miały być zamontowane;
- początkowa pozycja wirników – wybierana przez operatora, odmienna dla każdej wiadomości;
- ustawienie wirników – pozycja w jakiej należało ustawić pierścienie alfabetyczne w zależności od okablowania wirników;
- ustawienie łącznicy kablowej – schemat połączenia wtyczek na łącznicy kablowej;
- sposób okablowania walca odwracającego (w późniejszych wersjach).

Enigma została zaprojektowana w taki sposób, że transmisja musiała być bezpieczna także w przypadku gdy sposób okablowania wirników był znany dla podsłuchującego, w praktyce jednak dane na temat okablowania wirników były tajne (Kozaczuk, 1984). Użytkownicy Enigmy byli pewni, że bezpieczeństwo przekazu jest całkowite ze względu na olbrzymią liczbę możliwych kombinacji ustawień maszyny, a jedyną metodą rozkodowania wiadomości jest atak metodą *brute force*.

Większość kluczy obowiązywała przez określony czas, przeważnie jeden dzień, jednak do szyfrowania każdej wiadomości wirniki były ustawiane indywidualnie (Kozaczuk, 1984). Postępowano tak dlatego, że duża liczba przekazów zaszyfrowanych w ten sam lub podobny sposób stanowiła doskonały materiał dla kryptologów do analizy częstościowej i łatwiejszego złamania szyfru (Kozaczuk, 1984). Związane to było także z tym, że typowa depesza wojskowa na początku zawierała identyfikator (zwykle kryptonim) nadawcy.

Powodowało to, że w przypadku nadawców przesyłających dużą liczbę depesz (np. sztabów wysokiego szczebla) otrzymywano dużą liczbę depesz o identycznym początku (zaszyfrowany identyfikator nadawcy, który wywiad przeciwnika zwykle znał), co mogło ułatwić atak kryptologiczny. Aby temu przeciwdziałać dla każdej wiadomości wprowadzano indywidualne ustawienia, podobnie jak we współczesnej kryptografii stosuje się wektor startowy. Zaszyfrowana właściwa pozycja wirników była transmitowana tuż przed głównym szyfrogramem (Kozaczuk, 1984). Procedura ta, nazywana procedurą wstępną, choć miała podnieść bezpieczeństwo, to przez błędy

szyfrantów niemieckich pozwoliła na złamanie pierwszych wersji Enigmy (vide Rozdział 2.3.4).

Enigma wykorzystywana w wojsku używała tylko dwudziestosześcioliterowego alfabetu (Kozaczuk, 1984). Znaki przestankowe zastępowane były przez rzadko występujące sekwencje liter. Spacja była zwykle pomijana lub zastępowana literą X, która była też używana jako kropka lub przecinek dziesiętny (Kozaczuk, 1984). Niektóre znaki były różnie wykorzystywane przez różne siły zbrojne, np. siły lądowe i Luftwaffe zamiast przecinka wykorzystywały ZZ, a zamiast znaku zapytania – frazę FRAGE lub FRAQ (Kozaczuk, 1984). Marynarka wojenna z kolei zamiast przecinka wykorzystywała literę Y a zamiast znaku zapytania – UD (Kozaczuk, 1984). Litery CH, jak w wyrazie *Acht* (osiem) lub *Richtung* (kierunek) były zastępowane przez Q (AQT, RIQTUNG). Dwa, trzy lub cztery zera zastępowane były przez odpowiednio: CENTA, MILLE oraz MYRIA (Kozaczuk, 1984).

Różne grupy użytkowników Enigmy stosowały rózny sposób przesyłania wiadomości: siły lądowe i Luftwaffe robiły to w postaci pięcioliterowych grup, zaś marynarka wojenna – grup czteroliterowych (Kozaczuk, 1984).
Dodatkowo, maskowano najczęściej używane słowa pisząc je na różne sposoby (Kozaczuk, 1984).

Aby dodatkowo utrudnić pracę kryptologom wprowadzono ograniczenie długości meldunku do 250 znaków (Kozaczuk, 1984). Dłuższe przekazy dzielono na części, z których każda miała swój własny klucz wiadomości (Kozaczuk, 1984).

2.4.4 Złamanie szyfru Enigmy

Krótko po odzyskaniu niepodległości w 1918 w formującej się armii polskiej zorganizowano komórkę, której zadaniem było przechwytywanie i czytanie meldunków armii sąsiadujących krajów. Wykonaniem tego zadania zajął się znający kilka języków obcych porucznik Jan Kowalewski (Fot. 2.16) (Nowik, 2004).

Pierwsze szyfry sowieckie złamał używając analizy częstotliwościowej, której nauczył się z opowiadania Edgara Allana Poe *Złoty żuk* (Nowik, 2004).
Utworzone przez Kowalewskiego Biuro Szyfrów działało w ramach tzw. II Wydziału (wywiadu wojskowego).

Fot. 2.16. Jan Kowalewski
(na zdjęciu w stopniu majora, jako attaché wojskowy w Moskwie)
(źródło: Nowik, 2004)

Praca polskich kryptologów doprowadziła między innymi do odkrycia luk w lewym skrzydle Armii Czerwonej, co umożliwiło Marszałkowi Józefowi Piłsudskiemu zwycięstwo po uderzeniu w to skrzydło w sierpniu 1920 roku podczas Bitwy warszawskiej (Nowik, 2004).

Odkrycie archiwum Biura Szyfrów w kilkadziesiąt lat po wojnie polsko-bolszewickiej wykazało, że wywiad radiowy w latach 1919–1920 był najbardziej kompletnym i współczesnym wywiadem, jeśli chodzi o wszelakie informacje dotyczące funkcjonowania Armii Czerwonej, a w szczególności jednostek działających na froncie. Wywiad radiowy w dużym stopniu wpłynął na przebieg wszystkich działań wojennych przeprowadzonych przez Polskę w 1920 roku (Nowik, 2004).

Do 1926 roku regularnie odczytywano nieskomplikowane kody niemieckie i sowieckie, gdyż żadne z tych państw nie stosowało dotychczas kodów maszynowych

(Garliński, 1999). Sytuacja uległa pogorszeniu w lipcu 1928 roku, gdy meldunki niemieckich sił lądowych stały się dla polskich służb specjalnych zagadką.

Metodami statystycznymi ustalono, że nowy szyfr jest szyfrem maszynowym. Ponadto dzięki przypadkowi w styczniu 1929 roku udało się sfotografować zawartość jednej z paczek na warszawskim lotnisku Okęcie (Garliński, 1999).

Podejrzenie celników wzbudziło dziwne zachowanie pracownika ambasady niemieckiej, żądającego natychmiastowego zwrotu przesyłki zaadresowanej do filii jednego z niemieckich przedsiębiorstw na terenie Polski. Zawartością przesyłki okazała się cywilna Enigma (Garliński, 1999).

Wydarzenia te doprowadziły do zakupu i sprowadzenia do kraju handlowej wersji Enigmy. Intensywne badania cywilnej wersji maszyny oraz próby rozwiązania przechwyconych niemieckich meldunków, prowadzone między innymi przez kapitana Maksymiliana Ciężkiego (Fot. 2.17) i porucznika Wiktora Michałowskiego, nie przyniosły żadnych pozytywnych rezultatów.

W tej sytuacji jeszcze w styczniu 1929 roku na zlecenie Sztabu Głównego Wojska Polskiego w Instytucie Matematyki Uniwersytetu Poznańskiego zorganizowano kurs kryptologii (Garliński, 1999).

Kurs ten, prowadzony przez majora Pokornego, kapitana Ciężkiego i inżyniera Pallutha miał za zadanie wyłowić wyróżniających się w tym kierunku studentów matematyki. Podczas jednych zajęć, kapitan Ciężki dał adeptom kryptologii zadanie rozwiązania – złamanego już wcześniej przez niego samego – transpozycyjnego kodu niemieckiego (Kozaczuk, 1984).

Spośród uczestników kursu wybrano ostatecznie 8 studentów. Byli to między innymi wyróżniający się Marian Rejewski (Fot. 2.18a), Jerzy Różycki (Fot. 2.18b) i Henryk Zygalski (Fot. 2.18c). Rozpoczęli oni pracę nad niemieckimi szyframi w Komendzie Miasta w Poznaniu (Kozaczuk, 1984).

fot. 2.17. Maksymilian Ciężki
(źródło: Kozaczuk, 1984)

Fot. 2.18. a) Marian Rejewski
b) Jerzy Różycki
c) Henryk Zygalski
(źródło: Kozaczuk, 1984)

Materiały do deszyfracji pochodziły głównie ze stacji nasłuchowej pod Poznaniem, ale także z Warszawy, Stargardu Gdańskiego i Krzesławic pod Krakowem. Placówka Biura Szyfrów w Poznaniu, pomyślana jako tymczasowa, została rozwiązana, a trzem najbardziej wyróżniającym się pracownikom: Rejewskiemu, który w tym czasie wykładał matematykę na Uniwersytecie Poznańskim oraz świeżo upieczonym absolwentom tej uczelni: Różyckiemu i Zygalskiemu, zaproponowano stałą pracę w Biurze Szyfrów Sztabu Głównego Wojska Polskiego w Warszawie.

Pierwszym sukcesem grupy młodych kryptologów było odczytanie czteroliterowego kodu niemieckiej marynarki wojennej (Kozaczuk, 1984). Dostrzegając ogromne możliwości, udostępniono Marianowi Rejewskiemu zbierane w ostatnich latach szyfrowane maszynowo niemieckie meldunki i zlecono ich przeanalizowanie. Przystępując do łamania Enigmy, Polacy wiedzieli że zawiera ona element nieobecny w wersji handlowej oraz że każda depesza kodowana jest indywidualnym kluczem (Garliński, 1999).

Rejewski, dysponujący handlową wersją Enigmy i depeszami niemieckimi, zauważył występowanie pewnych charakterystycznych cech, które ujął w postać układu równań permutacyjnych (Garliński, 1999). I mimo, iż ilość niewiadomych wykluczała rozwiązanie równań, to sam fakt wykorzystania wyższej matematyki stał się pierwszym w tym czasie i przełomowym elementem w rozwiązywaniu problemów szyfrów maszynowych, czyniąc Rejewskiego „ojcem" nowoczesnych ataków kryptograficznych.

Widząc ogromne możliwości dalszych postępów w próbie rozwiązania szyfru Enigmy, kierownik Biura Szyfrów – następca majora Pokornego – major Gwidon Langer przekazał Rejewskiemu cztery dokumenty zdobyte przez wywiad francuski (Garliński, 1999). Było to: zdjęcie wojskowej odmiany Enigmy, instrukcja obsługi Enigmy oraz dwie, nieaktualne od roku tabele kluczy. Jak obecnie stwierdzają historycy, informacje zawarte w tych dokumentach nie były wystarczające do odkrycia największej zagadki Enigmy: wewnętrznych połączeń wirników, jednak w znacznym stopniu pomogły Rejewskiemu w zlikwidowaniu kilku niewiadomych z równań permutacyjnych.

W 1931 roku kapitan Gustave Bertrand, szef Służby Wywiadowczej, ze względu na niezdolność francuskich służb kryptograficznych do rozwiązania szyfru maszynowego, postanowił nawiązać współpracę pomiędzy wywiadem francuskim i polskim (Garliński, 1999).

Już podczas pierwszej swojej wizyty w Warszawie, przekazał on wspomniane dokumenty Polakom. Dokumenty te oraz kolejne materiały przekazywane w później, pochodziły od płatnego szpiega noszącego pseudonim Asché.

Asché, czyli Hans-Thilo Schmidt pracował jako urzędnik w niemieckim Centrum Szyfrów, zajmując się niszczeniem zdezaktualizowanych tabeli kluczy (Garliński, 1999). Sprzedał on wywiadowi francuskiemu wiele mniej lub bardziej ważnych dokumentów, które z kolei przekazywane były szefom polskiego Biura Szyfrów. Jednakże żaden z późniejszych dokumentów nie został udostępniony Rejewskiemu lub zespołowi kryptologów.

Czym tłumaczyć fakt ukrycia posiadanych tabeli kluczy?

Można przypuszczać, że strategia kierownictwa wiązała się z potrzebą wyrobienia silnego zespołu kryptologów, który mógłby odnosić sukcesy z niemieckimi szyframi również w przypadku, gdyby nagle zabrakło materiałów wywiadowczych (liczono się z nagłym przerwaniem działalności Asché, jak i z możliwością zrezygnowania Francji ze współpracy).

Największym osiągnięciem Rejewskiego było wydedukowanie połączeń wewnętrznych jednego z wirników Enigmy. Założył on, że w analizowanych fragmentach tekstu będzie się obracał wyłącznie pierwszy wirnik, co okazało się być słuszne w około 80% przypadków (Garliński, 1999). W tym przypadku nieznane były: sekwencja połączeń styków walca odwracającego, sposób okablowania pierwszego wirnika (sekwencja połączeń styków znajdujących się na obu stronach wirnika), oraz kolejność liter w wirnikach (26 liter na każdym wirniku). Ustawienia łącznicy otrzymał od francuskiego wywiadu, założył również alfabetyczną kolejność liter w wirnikach; w tym przypadku sposób okablowania wirnika pozostał jedyną niewiadomą (Garliński, 1999). Dane wywiadu dotyczyły dwóch różnych kwartałów (okresów).

Ponieważ Niemcy zmieniali ustawienia wirników (kolejność 3 wirników na wspólnej osi) co kwartał, analogiczną metodą rozwiązano kwestię sposobu okablowania drugiego wirnika (Garliński, 1999). Mając te dane udało się następnie odtworzyć

sposób okablowanie wirnika trzeciego oraz walca odwracającego. W ostatnich dniach 1932 roku Rejewski odszyfrował pierwszą depeszę Enigmy (Garliński, 1999).

Jedna z pierwszych procedur wstępnych została wykorzystana przez polskich kryptologów do pierwszego złamania szyfru Enigmy. Polegała ona na ustawieniu wirników zgodnie z kluczem dziennym odczytanym z książki kodowej (Garliński, 1999). Początkowe ustawienie wirników mogło mieć postać AOH i taką kombinację ustawiał operator. Następnie wybierano przypadkową kombinację ustawień wirników np. EIN, która stawała się indywidualnym kluczem wiadomości. Klucz wiadomości był wpisywany dwukrotnie (w celu uniknięcia błędów) jako EINEIN i po zaszyfrowaniu mógł mieć postać XHTLOA, którą nadawano na początku przekazu szyfrowanego. Po nadaniu klucza operator ustawiał wirniki maszyny w pozycji EIN i rozpoczynał wpisywanie wiadomości do zaszyfrowania.

Procedura odbiorcza była operacją odwrotną (Garliński, 1999). Najpierw w maszynę ustawioną zgodnie z kluczem dziennym wpisywano pierwszą odebraną sekwencję znaków XHTLOA, która po rozkodowaniu dawała indywidualny klucz szyfrogramu EINEIN. Następnie operator ustawiał wirniki Enigmy w pozycję EIN i przystępował do dekodowania właściwego przekazu.

Pierwszym błędem procedury wstępnej było nadawanie w początkowym okresie używania Enigmy indywidualnego klucza wiadomości tekstem otwartym (Garliński, 1999). Drugim błędem natomiast było konstruowanie klucza wiadomości z trzech znaków powtórzonych dwukrotnie (Garliński, 1999), co pozwoliło na odkrycie relacji pomiędzy pierwszym i czwartym znakiem, drugim i piątym, oraz trzecim i szóstym. Oba te niedostateczne zabezpieczenia transmisji pozwoliły pracownikom polskiego Biura Szyfrów na odtworzenie działania Enigmy i dekodowanie wiadomości przesyłanych przy użyciu przedwojennych maszyn szyfrujących.

Inne błędy szyfrantów niemieckich związane z tą procedurą to (za: Kozaczuk, 1984):

- stosowanie klucza stanowiącego powtórzenie tej samej litery (np. AAA);
- stosowanie klucza złożonego z liter leżących w alfabecie obok siebie (np. ABC) lub leżących obok siebie na klawiaturze;
- stosowanie klucza będącego wyrazem w języku niemieckim;

- stosowanie w wielu depeszach tego samego klucza np. inicjałów szyfranta, jego bliskiej osoby, etc.

W 1940 zmieniono procedurę wstępną zwiększając bezpieczeństwo szyfrów. Książki kodowe zawierały tylko dane na temat zestawu wirników i ich wzajemnego ułożenia, bez kluczy dziennych (Kozaczuk, 1984).

Dla każdej wiadomości operator wybierał przypadkowe ustawienie początkowe wirników, np. WZA i przypadkowy klucz wiadomości np. SXT. Po ustawieniu wirników Enigmy w położenie WZA wpisywał klucz wiadomości SXT otrzymując przykładowo ciąg znaków UHL. Następnie ustawiał wirniki maszyny w położenie SXT i kodował resztę informacji. Transmitowany meldunek rozpoczynał się od ciągu znaków mówiącego o ustawieniu początkowym WZA, następnie zakodowanego klucza wiadomości UHL a następnie właściwej treści szyfrogramu.

Odbierający wiadomość operator wykonywał operacje odwrotne: najpierw ustawiał wirniki w pozycję WZA i dekodował z ciągu UHL klucz wiadomości SXT. Następnie ustawiał maszynę zgodnie z kluczem SXT i deszyfrował przekaz. Ta procedura wstępna była znacznie bezpieczniejsza niż przedwojenne, ponieważ nie zawierała podwójnej sekwencji znaków.

Powyższa procedura była wykorzystywana tylko przez siły lądowe i Luftwaffe, Kriegsmarine posiadała własne znacznie bardziej złożone procedury (Garliński, 1999). Wiadomość przeznaczona do zakodowania musiała być wstępnie zakodowana na podstawie książki skrótów kodowych zawierającej tabele zamieniające całe sentencje i zwroty na czteroliterowe grupy liter (Kozaczuk, 1984). Uwzględniono każde możliwe wyrażenie i każdy temat wiadomości i sytuacji na morzu (Kozaczuk, 1984). Swoje kody posiadały operacje tankowania i zaopatrzenia na morzu, nazwy zatok, państw, broni, pogody, pozycji wrogich jednostek, czasu, współrzędnych itd. Celem przyjęcia takiego rozwiązania było nie tylko utrudnienie złamania szyfru, ale także umożliwienie przekazania jak największej informacji w formie jak najkrótszej depeszy – dzięki czemu zmniejszano ryzyko ustalenia pozycji okrętu przez przeciwnika na podstawie nasłuchu i radionamierzania.

Przed wybuchem II wojny światowej Polacy opracowali niezwykle efektywne metody deszyfrowania Enigmy, wykorzystując w tym celu w sposób nowatorski istniejące teorie kombinatoryczne tzw. cykli i transpozycji.

Do określania permutacji cykli wirników Enigmy wykorzystywano zaprojektowany przez Rejewskiego i Różyckiego cyklometr i karty charakterystyk, które ze względu na zmianę kodowania wprowadzoną w 1938 przestały być wykorzystywane.
Do tego czasu ustalenie kodu dziennego przy pomocy powyższych narzędzi zajmowało około 15 minut (Garliński, 1999).

Około października 1938 Rejewski opracował kolejne elektromechaniczne urządzenie nazwane bombą kryptologiczną, którego zadaniem było automatyczne łamanie szyfru Enigmy w oparciu o opracowaną teorię cykli (Garliński, 1999). Bomba kryptologiczna składała się z sześciu sprzężonych polskich kopii Enigmy napędzanych silnikiem elektrycznym (Garliński, 1999).

W połowie listopada tego samego roku zbudowano sześć takich bomb, wykorzystywanych wyłącznie do rozszyfrowywania podwójnie szyfrowanych kluczy dziennych, nigdy zaś do dekodowania samych szyfrogramów, które dekodowano przy pomocy perforowanych płacht Zygalskiego (Rys. 2.19), opracowanych w celu znajdowania właściwego położenia wirników Enigmy (Garliński, 1999).
Jedna bomba kryptologiczna pozwalała na odkodowanie klucza dziennego w ciągu około dwóch godzin.

W połowie grudnia 1938 roku Niemcy dodali do zestawu dwa dodatkowe wirniki, co spowodowało, iż do rozwiązywania szyfru Polacy potrzebowali dziesięć razy więcej czasu. Wykonanie sześćdziesięciu Bomb przekraczało jednak techniczne i finansowe możliwości Biura Szyfrów, tym bardziej, że równocześnie należałoby wykonać, co najmniej 60 płacht Zygalskiego (Kozaczuk, 1984).

Z tego powodu kierownictwo Biura Szyfrów zdecydowało się na zaaranżowanie spotkania z szefami wywiadów Francji i Wielkiej Brytanii (Garliński, 1999). Do pierwszego spotkania doszło w styczniu 1939 w Paryżu (Garliński, 1999). Podczas drugiego spotkania, które odbyło się w dniach 24-26 lipca 1939 roku w Warszawie, Polacy ujawnili aliantom mocno strzeżoną przez tyle lat tajemnicę Enigmy (Garliński, 1999).

Na lipcowe spotkanie przybyli (za: Garliński, 1999) ze strony francuskiej: Gustave Bertrand i kapitan Henri Braquenie, ze strony angielskiej: szef Government Code and Cipher School komandor Alistair Denniston, główny kryptolog Alfred D. Knox oraz specjalista nasłuchu radiowego, komandor Humphrey Sandwith. Stronę polską

reprezentowali: szef Biura Szyfrów, Stefan Mayer, major Gwidon Langer i kapitan Ciężki oraz Rejewski, Różycki i Zygalski. Ciekawostką jest, że rozmowy prowadzono po... niemiecku, gdyż był to jedyny język znany wszystkim stronom (Garliński, 1999). Sojusznikom przekazano po jednej kopii Enigmy i komplecie innych materiałów.

Gdy 1 września 1939 roku wojska niemieckie napadły na Polskę, pracownicy Biura Szyfrów zostali ewakuowani przez Rumunię do Francji, by kontynuować prace we francuskim ośrodku kryptologicznym Bruno w Château de Bois-Vignolles koło Paryża (Kozaczuk, 1984).

Po kapitulacji Francji na terenie administrowanym przez rząd Vichy w willi Domaine les Fouzes w miejscowości Uzès powoli odbudowano ośrodek kryptologiczny, któremu nadano nazwę Cadix. W Algierze pozostała filia tego ośrodka, którą kierował major Maksymilian Ciężki. Co kilka miesięcy kryptolodzy z obu ośrodków wymieniali się, podróżując drogą morską z Francji do Algieru. Podczas jednej z takich wypraw w katastrofie statku Lamoriciere zginęło trzech polskich pracowników ośrodka Cadix. Był wśród nich Jerzy Różycki (Garliński, 1999).

Po wkroczeniu Niemiec do południowej Francji w listopadzie 1942 zaistniała konieczność ewakuowania ośrodka Cadix. Rejewski i Zygalski w styczniu 1943 przedostali się przez granicę francusko-hiszpańską, ale w Hiszpanii prawie natychmiast zostali aresztowani przez tamtejszą policję. Ostatecznie dzięki wstawiennictwu Polskiego Czerwonego Krzyża obaj kryptolodzy zostali 4 maja uwolnieni i odesłani do Madrytu. Następnie przedostali się do Portugalii, skąd ostatecznie trafili do Wielkiej Brytanii, gdzie 16 sierpnia rozpoczęli pracę w jednostce radiowej Sztabu Naczelnego Wodza Polskich Sił Zbrojnych w Stanmore-Boxmoor pod Londynem, gdzie pracowali do zakończenia wojny (Garliński, 1999).
Pozostali członkowie przedwojennego Biura Szyfrów – pułkownik Gwidon Langer i major Maksymilian Ciężki – zostali złapani przez Niemców i wysłani do oflagu Schloss-Eisenberg (Garliński, 1999).

Dzięki pracy kryptologów polskich, a później także brytyjskich z Blechley Park, oraz dzięki przechwyconym w międzyczasie egzemplarzom Enigmy, pod koniec wojny praktycznie cała korespondencja szyfrowana przy jej pomocy była odczytywana przez aliantów.

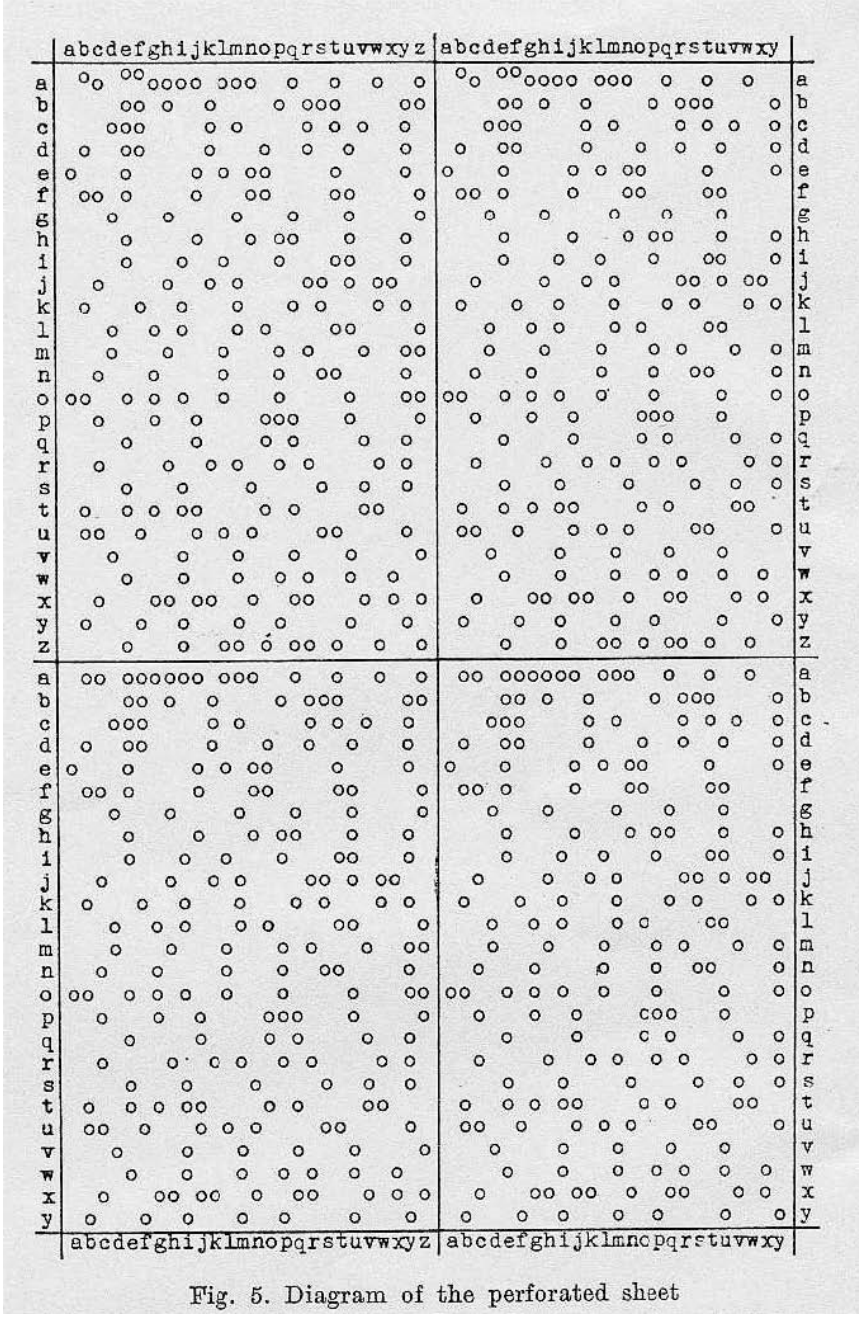


Fig. 5. Diagram of the perforated sheet

Rys. 2.19. Diagram jednej z płacht Zygalskiego
(źródło: Rejewski, 1980)

2.5 KRYPTOGRAFIA SYMETRYCZNA – TECHNIKI UŻYWANE WSPÓŁCZEŚNIE

2.5.1 SZYFRY BLOKOWE

Szyfr blokowy to najczęściej symetryczny kod korekcyjny, który potrafi zaszyfrować blok danych o określonej długości. Kody blokowe najczęściej określa się symbolem (n,k) – gdzie n określa długość słowa kodowego, zaś k – długość części informacyjnej (Knudsen & Robshaw, 2011).

Kody te służą do szybkiego wykrycia i korekcji błędów występujących podczas przesyłu danych cyfrowych. Informacje dzielone są w tych kodach na bloki, do których dołączana jest nadmiarowa część kodowa pozwalająca na detekcję błędów występujących w blokach oraz korekcję – w zależności od sposobu zaprojektowania kanału transmisji ponowne pobranie całego bloku lub dokonanie automatycznej korekcji (Knudsen & Robshaw, 2011).

Kody blokowe podzielić możemy na dwie najczęściej używane klasy: kody liniowe i wywodzące się z nich kody cykliczne.

Typowe rozmiary bloku oraz kluczy (te dwa rozmiary nie muszą być identyczne) to 64, 128, 192 lub 256 bitów, przy czym klucze mniejsze od 1024 bitów nie zapewniają współcześnie odpowiedniego poziomu bezpieczeństwa (Knudsen & Robshaw, 2011).

Szyfry blokowe stanowią podstawę wielu używanych współcześnie symetrycznych algorytmów szyfrujących.

DES oraz 3DES

Jednym z najpopularniejszych, używanym do dziś algorytmem szyfrujących jest Data Encryption System (DES), opracowany w latach 70.tych XX wieku w laboratoriach firmy IBM (Schneier, 2002).

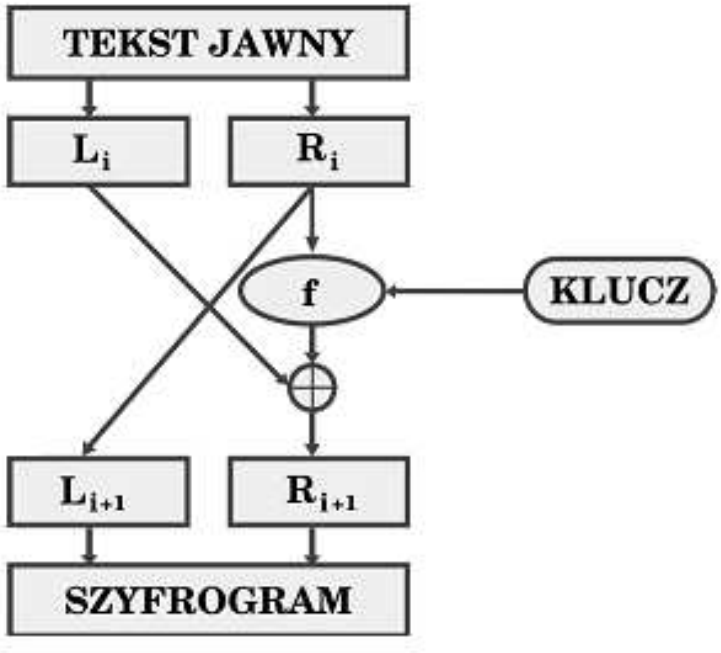
Od 1976 do 2001 roku stanowił standard federalny USA, a od roku 1981 standard ANSI dla sektora prywatnego (znany jako Data Encryption Algorithm).

Od kilku lat uznawany jest za algorytm niezapewniający odpowiedniego bezpieczeństwa, głównie ze względu na niewielką długość klucza (56 bitów), która sprawia, że jest bardzo podatny na atak siłowy (Schneier, 2002).

DES jest przykładem iterowanego szyfru blokowego. Algorytm ten korzysta z tzw. sieci Feistela, która pozwala na szyfrowanie i deszyfrowanie informacji tym samym algorytmem, mimo iż funkcja f nie jest odwracalna (Pieprzyk, Hardjono & Seberry, 2006).

Sieć Feistela generuje z tekstu jawnego szyfrogram, a z szyfrogramu tekst jawny. W ten sposób konstruowanie algorytmów szyfrujących znacznie się uprościło, ponieważ kryptografowie nie muszą troszczyć się o odwracalność funkcji f (Bishop, 2004).

Przykładowy schemat działania sieci Feistela został przedstawiony na Rysunku 2.20.



Rys. 2.20. Przykładowy schemat działania sieci Feistela (źródło: Wikimedia Commons)

Idea, o jaką opiera się algorytm jest bardzo prosta: tekst jawny jest dzielony na dwa równe bloki L_i oraz R_i. Funkcja f jest właściwym algorytmem szyfrującym – jako jej wynik otrzymywany jest szyfrogram, zaś i – jest numerem kolejnej rundy – co oznacza, że wynik jest ponownie kodowany i razy, co polepsza jakość szyfrowania.

Deszyfrowanie polega na zastosowaniu tych samych operacji w odwrotnej kolejności (różni się od szyfrowania tylko wyborem podkluczy, który teraz odbywa się od końca). DES ma 4 słabe i 12 półsłabych kluczy (NIST, 1995).

Kluczem słabym nazywany jest klucz kryptograficzny, który powoduje wygenerowanie identycznego podklucza w kolejnych krokach algorytmu szyfrującego (Knudsen & Robshaw, 2011).

W przypadku DES są to (za: Knudsen & Robshaw, 2011):

- wektor samych 1;
- wektor samych 0;
- pierwsza połowa wektora złożona z 1, zaś druga z 0;
- pierwsza połowa wektora złożona z 0, zaś druga z 1.

Mianem **klucza półsłabego** określany jest klucz kryptograficzny, dla którego istnieje inny, równoważny klucz .

W algorytmie DES szansa na wylosowanie któregokolwiek z tych kluczy wynosi (za: Knudsen & Robshaw, 2011)

$$(4+12/2^{56})=2,22*10^{-16}$$

co nie wpływa w istotny sposób na siłę szyfru.

Z powodu słabości klucza (56 bitów) DES został w dużej mierze zastąpiony przez inne szyfry: swoje własne modyfikacje, takie jak 3DES czy DESX, a także przez nowsze i bezpieczniejsze algorytmy jak AES czy IDEA (Schneier, 2002).

Przykładowo, 3DES to algorytm polegający na zaszyfrowaniu wiadomości za pomocą algorytmu DES trzykrotnie:

- wiadomość szyfrowana jest pierwszym kluczem;
- wiadomość deszyfrowana jest drugim kluczem;
- wiadomość szyfrowana jest za pomocą trzeciego klucza.

Tak więc, proces szyfrowania można zapisać następująco:

$$C = E_3(D_2(E_1(P)),$$

gdzie: P – tekst jawny wiadomości, C – szyfrogram, E – funkcja szyfrująca, D – funkcja deszyfrująca.

Użycie deszyfrowania w drugim kroku nie wpływa na siłę algorytmu (deszyfrowanie w DES jest identyczne jak szyfrowanie, tylko ma odwróconą kolejność rund), ale umożliwia – w razie konieczności – użycie 3DES w trybie kompatybilności z DES – za klucz pierwszy i drugi (lub drugi i trzeci) przyjmowany jest dowolny taki sam klucz, zaś za ostatni zwykły klucz DES (Knudsen & Robshaw, 2011):

$$C = E_3(D_1(E_1(P)) = E_3(P)$$

$$C= E_3(D_3(E_1(P)) = E_1(P)$$

3DES używa takich samych rozmiarów bloków oraz trybów jak zwykły DES.

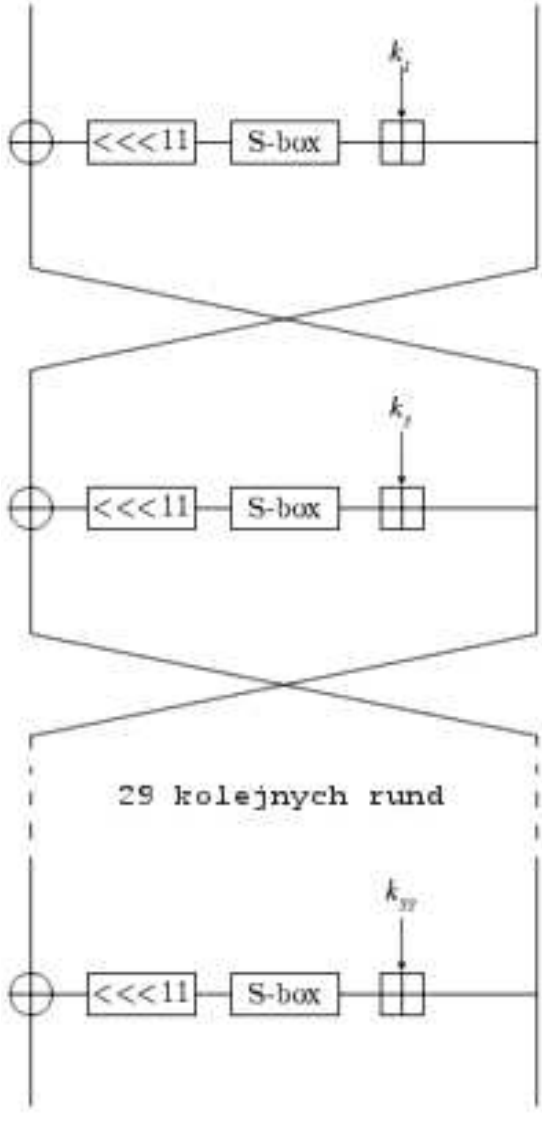
3DES z trzema różnymi kluczami (3TDES) ma siłę 168 bitów (trzykrotne szyfrowanie DES kluczem 56-bitowym), jednak zostało udowodnione, że rzeczywista moc klucza 3DES jest równa 112 bitom ze względu na podatność na atak typu Meet-in-the-Middle (Knudsen & Robshaw, 2011).

GOST 28147–89

GOST 28147–89 (pełna nazwa *Gousudarstviennyj Standard 28147-89*) jest stosowanym cywilnie od 1990 roku nietajnym standardem szyfrowania przyjętym najpierw przez ZSRR, a następnie przez Wspólnotę Niepodległych Państw.

GOST 28147–89 uwzględnia wszystkie poznane do 1989 roku wady DES. Jego budowa cechuje się swoistą oryginalnością, posiada bowiem tajne bloki. GOST 28147–89 jest bitowym szyfrem blokowym, używającym 256.bitowego klucza, zrealizowanego w postaci ośmiu 32.bitowych podkluczy (Garbarczuk & Świć, 2005).

Procedury szyfrowania i deszyfrowania odpowiadają interaktywnemu schematowi Feistela, w którym funkcja F(R,K) zdawana jest przez operację sumowania modulo 2^{32}, podstawienia tablicowe realizowane nad czterobitowymi blokami i operacje przesunięcia cyklicznego na 11 bitów, wykonywane na 32.bitowym podblokiem (Garbarczuk & Świć, 2005). Schemat działania GOST 28147–89 został przedstawiony na rysunku 2.21.



Rys. 2.21. Schemat działania GOST 28147–89
(źródło: Garbarczuk & Świć, 2005)

Zgodnie z normatywną dokumentacją tablice podstawień służą jako dodatkowy klucz (ok. 512 bitów) i powinny być tajne. Ten dodatkowy klucz jest ogólny dla wszystkich użytkowników danego systemu i jest dostarczany w odpowiednim porządku – wynika to z faktu, że trwałość krytyczna GOST 28147–89 zależy

od jakości stosowanych tablic podstawień i tajnego bloku. Przy prawidłowym wyborze nawet w przypadku znanych tablic podstawienia standard gwarantuje wysoką odporność. Należy podkreślić, że kryteria wyboru tablic dla tego szyfru nie są przytaczane w oficjalnych dokumentach (Garbarczuk & Świć, 2005). Wymóg tajności tablic podstawień nie jest zgodny z zasadą Kerckhoffsa, ponieważ dane elementy szybciej odnoszą się do algorytmu szyfrowania, niż do tajnego klucza, możliwego do zmiany w łatwy sposób (Garbarczuk & Świć, 2005).

Podstawową wadą GOST 28147–89 jest mała prędkość przy realizacji programowej, co związane jest ze stosowaniem dużej liczby operacji podstawiania w czterobitowym bloku (Garbarczuk & Świć, 2005). W porównaniu do DES, GOST 28147–89 używa w kolejnych rundach relatywnie prostej funkcji. Należy jednak zauważyć, że udało się zrekompensować jej prostotę poprzez realizację algorytmu w oparciu o 32 rundy i tajne bloki (Garbarczuk & Świć, 2005).

W latach 2011 oraz 2012 pojawiły się informacje o wykryciu licznych luk w GOST 28147-89, które umożliwiają przeprowadzenie ataku na pełnym 32-rundowym szyfrogramie. Autorami niektórych z metod ataków są polscy kryptolodzy, m.in. Nicolas Tadeusz Courtois, przedstawiony na fotografii 2.21 (Courtois, 2011).

Fot. 2.21. Nicolas Tadeusz Courtois
(źródło: http://nicolascourtois.me.uk)

IDEA

International Data Encryption Algorithm (IDEA) to zaprojektowany w 1991 roku symetryczny szyfr blokowy posiadający 128-bitowy klucz i operujący na 64-bitowych blokach wiadomości (Schneier, 2002).

IDEA używa 3 rodzajów operacji na 16-bitowych liczbach. Są to (za: Schneier, 2002):

- XOR (alternatywa wykluczająca);
- dodawanie modulo 2^{16};
- mnożenie modulo $2^{16} + 1$ (które jest liczbą pierwszą), przy czym liczba 0 jest traktowana jako 2^{16}.

Warto zauważyć, że IDEA była używana we wczesnych wersjach PGP i jest dostępna jako opcjonalny algorytm w OpenPGP. Ze względów patentowych oraz ze względu na powstanie lepszych algorytmów (np. opisany poniżej AES), a także postępy w kryptoanalizie IDEA znacznie straciła na popularności, choć należy odnotować, że nigdy nie została złamana (Schneier, 2002).

Patenty dotyczące IDEA wygasły w 2012, tak więc szyfr ten jest dostępny dla każdego bez żadnych opłat.

AES (Rijndeal)

Advanced Encryption Standard (AES, znany również pod nazwą kodową Rijndael) to symetryczny szyfr blokowy przyjęty przez amerykański Narodowy Instytut Standardów i Technologii w roku 1997 jako następca algorytmu DES (Knudsen & Robshaw, 2011).

Algorytm ten umożliwia użycie kluczy o długościach 128, 192 i 256 bitów i operuje na blokach danych o długości 128 bitów (oryginalna specyfikacja Rijndael dopuszczała również bloki o rozmiarze 192 i 256 bitów) (Knudsen & Robshaw, 2011).

AES wykonuje 10 (przy użyciu standardowego klucza o długości 128 bitów), 12 (przy użyciu klucza o długości 192 bitów) lub 14 (przy kluczu 256.-bitowym) rund szyfrujących składających się z następujących kroków: substytucji wstępnej, permutacji macierzowej (mieszanie wierszy, mieszanie kolumn) i modyfikacji za pomocą klucza (Schneier, 2002).

Funkcja podstawieniowa ma bardzo oryginalną konstrukcję, która uodparnia ten algorytm na znane ataki kryptoanalizy różnicowej i liniowej. Od 2001 stanowi standard federalny USA (Knudsen & Robshaw, 2011).

Serpent

Serpent jest symetrycznym szyfrem blokowym stworzonym przez Rossa Andersona, Eliego Bihama i Larsa Knudsena. Na konkursie AES szyfr ten zajął drugie miejsce, zaraz po Rijndaelu. Serpent jest wolniejszy od laureata konkursu, jednak równocześnie bardziej bezpieczny.

Serpent operuje na blokach o rozmiarach 128 bitów oraz na kluczu o długościach: 128, 192 lub 256 bitów. Korzysta on z 32 rund, w trakcie których następuje przekształcenie przez XOR względem klucza rundy, użycie 128.-bitowej funkcji mieszającej i zastosowanie 32 czterobitowych S-boxów (Knudsen & Robshaw, 2011).

Dzięki użyciu w S-boxach wyłącznie funkcji boolowskich algorytm zyskuje znacznie na szybkości. W przypadku zwykłej implementacji konieczne byłoby przejrzenie w każdej z 32 rund trzydziestu dwóch S-boxów, co oznaczałoby konieczność przejrzenia w sumie 1024 S-boxów.

W Serpencie każdy z czterech bitów wynikowych tych S-boxów jest wyrażany w postaci funkcji boolowskiej czterech bitów wejściowych. Dodatkowo w 32-bitowych procesorach można przetwarzać transformacje na wszystkich trzydziestu dwóch S-boxach jednocześnie, gdyż każdy bit wynikowy opisany jest taką samą funkcją, choć działającą na różnych danych wejściowych (Schneier, 2002).

Twofish

Algorytm Twofish jest zbudowany na zasadzie prawie czystej sieci Feistela. Twofish jest standardem otwartym, nie objętym żadnymi patentami i do tej pory nie został złamany poza metodą ataku brute force.

W kryptografii Twofish jest symetrycznym, blokowym kluczem szyfrującym. Operuje na blokach danych o wielkości 128 bitów i wykorzystuje klucze wielkości od 128 do 256 bitów. Najczęściej są stosowane klucze o długości 128, 192 oraz 256 bitów. Cechą charakterystyczną Twofish jest zastosowanie kluczujących S-boxów.

Blok danych wejściowych o długości 128 bitów dzielony jest na cztery części, z których każda złożona z 32 bitów jest poddawana operacji wybielenia (ang. *whiteninig*), czyli wykonaniu XOR pomiędzy czterema blokami danych (po 32 bity każdy) z czterema kluczami (także o długości 32 bity każdy).
Powoduje to zwiększenie siły algorytmu i utrudnienie złamania go.

Następnie dwie pierwsze części (R_0 i R_1) trafiają do funkcji F. Kolejne części (R_2 i R_3) są pozostawiane bez zmian. Funkcja F bierze dwie pierwsze części oraz dwa klucze i na ich podstawie generuje dwa wektory składające się w sumie z 64 bitów. Są one dalej łączone z wektorami R_2 i R_3 , XOR-owane z dwoma innymi kluczami oraz przesuwane bitowo w prawą lub lewą stronę.

Kolejnym etapem jest zamiana miejscami pary wektorów R_0 i R_1 z parą R_2 i R_3 oraz ponowne przejście przez funkcję F. Takie jedno wykonanie się funkcji F wraz z późniejszymi operacjami na jej wynikach oraz zamianie miejscami par wektorów jest określane mianem rundy algorytmu.

Na cały algorytm Twofish składa się 16 takich rund. W każdej z nich do funkcji F trafiają inne klucze – funkcja F jest najważniejszym elementem – sercem algorytmu. Po wykonaniu ostatniej rundy bloki R są ponownie XOR-owane z kluczami i podawane na wyjście jako zaszyfrowane bloki danych.

2.5.2 Szyfr książkowy

Szyfr książkowy to szyfr, w którym każda z liter tekstu jawnego wiadomości zastępowana jest liczbami oznaczającymi jej pozycję w ustalonym tekście, będącym kluczem do szyfru (Singh, 2003).
Istnieje również inna wersja tego szyfru, która polega na zastępowaniu całych słów ich pozycjami w książce (Schneier, 2002).

Przykładem pierwszego z wymienionych typów niech będzie słowo LASKOWSKI zaszyfrowane przy pomocy początkowego fragmentu Inwokacji z *Pana Tadeusza* Adama Mickiewicza.
Dla ułatwienia poszczególne litery tekstu wiadomości zostaną wytłuszczone.

Litwo! Ojczyzno moj**a**! ty jesteś jak zdrowie.
Ile cię trzeba cenić, ten tylko **s**ię dowie,
Kto cię stracił. Dziś pięk**n**o**ś**ć t**wą** w całej ozdobie
Widzę i opi**s**uję, bo tęs**k**nię po tob**i**e

Zakładając, że powyższy tekst znajdował się na pierwszej stronie książki, możemy go zaszyfrować np. przy użyciu trzech liczb. Pierwsza odpowiadać będzie numerowi strony (w niniejszym przykładzie będzie to zawsze 1), druga – numerowi wiersza, trzecia zaś – konkretnej literze w tym wierszu.
Oznacza to, że słowo LASKOWSKI przyjmie postać:

```
L   1-1-1
A   1-1-17
S   1-2-27
K   1-3-1
O   1-3-22
W   1-3-1
S   1-4-10
K   1-4-19
I   1-4-28
```

Szyfr książkowy jest jednym z najtrudniejszych szyfrów do złamania. Przy dobrze dobranym tekście stanowiącym podstawę szyfru praktycznie jedyną metodą odczytania wiadomości (bez znajomości klucza) jest atak metodą brute force, czyli wypróbowanie wszystkich możliwych kombinacji.

Jedną z najlepszych ilustracji mocy tego szyfru jest sprawa złota Thomasa J. Beale, który zaszyfrował przy pomocy szyfru książkowego informację o miejscu ukrycia skarbu (Singh, 2003). Od połowy XIX wieku, kiedy publicznie ujawniono szyfrogramy, udało się odczytać tylko jeden z nich, zaszyfrowany przy użyciu *Deklaracji Niepodległości USA*. Dwa pozostałe pozostają jak dotąd nieodczytane (Singh, 2003).

2.5.3 SZYFR Z KLUCZEM JEDNORAZOWYM

Szyfr z kluczem jednorazowym został opracowany w 1917 roku przez Gilberta Vernama (Kahn, 1997). Jest dużym zbiorem o niepowtarzalnych i przypadkowych sekwencjach znaków.

Każdy klucz używany jest tylko raz, do zaszyfrowania tylko jednej wiadomości. Klucz tworzony jest w sposób losowy, przeciwnik nie ma informacji, która może ułatwić złamanie szyfru.

Po zaszyfrowaniu wiadomości nadawca niszczy strony z wykorzystanym zbiorem znaków. Odbiorca dysponuje identycznym zbiorem i używa tych samych znaków zbioru do odszyfrowania każdego znaku szyfrogramu. Podobnie jak nadawca po odszyfrowaniu wiadomości niszczy zbiór znaków stanowiących klucz.

Przy nadawaniu nowej wiadomości trzeba zastosować nowy zbiór znaków i nowe znaki klucza (Schneier, 2002).

Szyfrowanie z kluczem jednorazowym może być rozszerzone na dane binarne. Zamiast zestawu znaków są stosowane klucze binarne.

Metoda tworzenia i użycia klucza kryptograficznego wymaga, aby były spełnione następujące warunki (za: Schneier, 2002):

- Klucz użyty do szyfrowania wiadomości był dłuższy lub równy szyfrowanej wiadomości;
- Klucz był wygenerowany w sposób całkowicie losowy (nie może istnieć sposób na odtworzenie klucza na podstawie znajomości działania generatorów liczb pseudolosowych);
- Klucz nie może być użyty do zaszyfrowania więcej niż jednej wiadomości.

Wykorzystanie tej metody w np. szyfrowaniu XOR, bądź w szyfrze polialfabetycznym zapewnia całkowite bezpieczeństwo wiadomości, ponieważ dla każdej pary P i C (wiadomość i tekst zaszyfrowany) istnieje pasujący do nich klucz, czyli znając jedynie C, możemy dopasować do niego dowolną wiadomość (P) o tej samej długości i na ich podstawie wyliczyć pasujący K.

Dzięki temu złamanie szyfru nie jest możliwe nawet poprzez testowanie wszystkich możliwych kluczy (Schneier, 2002).

Problem złamania tego szyfru jest podobny do problemu związanego z rozwiązaniem równania: M + K = C, w którym znane jest jedynie C.

Zakładając, że przeciwnik nie ma dostępu do jednorazowego zestawu znaków stosowanego do szyfrowania wiadomości, można powiedzieć, że jest to idealnie bezpieczny algorytm utajniania. Dowolny szyfrogram może być szyfrogramem dowolnego tekstu jawnego o tej samej długości (Schneier, 2002).

Praktyczną wadą algorytmu jest długość klucza, która nie może być mniejsza od długości wiadomości, jaką nadawca zamierza przesłać. Rutynowe stosowanie szyfrów z kluczem jednorazowym wymagałoby od nadawcy i odbiorcy wcześniejszego uzgodnienia ogromnego klucza (bądź ogromnego zbioru kluczy). Problem stanowi zarówno całkowicie losowe wygenerowanie klucza, jak i jego bezpieczne przekazanie drugiej stronie. Z tego powodu algorytm z kluczem jednorazowym znajduje zastosowanie przede wszystkim w szyfrowaniu wyjątkowo tajnych informacji w kanałach o małej przepustowości.

Przykładem może być tutaj tzw. gorąca linia między prezydentami Rosji i Stanów Zjednoczonych (Singh, 2003).

Innym interesującym przykładem mogą być tzw. **radiostacje numeryczne**, czyli stacje krótkofalowe o nieustalonym statusie i własności, nadające zazwyczaj zestaw liczb, słów, liter lub wyrazów alfabetu fonetycznego.

Głosy spikerów, z którymi można spotkać się słuchając tych stacji radiowych, nierzadko są generowane komputerowo przy użyciu syntezatora głosu i są czytane w wielu językach. Zwykle są to głosy żeńskie, ale czasami można usłyszeć także głosy męskie lub nawet dziecięce (Kahn, 1997).

Stacje nie są zarejestrowane w Międzynarodowym Związku Telekomunikacyjnym, więc ich działalność ma z punktu prawnego charakter piracki (Mason, 1991). Radiostacje te są wykorzystywane najprawdopodobniej w charakterze jednostronnego kanału łączności ze szpiegami pracującymi na odległych zakonspirowanych placówkach (Mason, 1991).

Część z radiostacji numerycznych pojawia się nagle i równie gwałtownie milknie, ale niektóre mają regularną "ramówkę". Ich działalność nasiliła się nieznacznie

na początku lat 90. XX wieku. Po definitywnym zakończeniu zimnej wojny aktywność stacji zmalała (Kahn, 1997).

Przykładowy zapis jednej z audycji stacji numerycznej Yankee Sierra (za: Mason, 1991):

```
Yankee Sierra Yankee Sierra Yankee Sierra Yankee Sierra
635 635 27 gruppen. 516 516 78 gruppen. Achtung, 635 63527 gruppen.
2690 2707 2745 3228 3262 4543 4594 4821 4888 5015 5182 5732 5770 6370
6765 6853
7404 7532 7661 7740 7752 7858 8063 8173 9040 9325 9450 10177 10460
10500 10740 11108
11545 11617 12092 12210 12314 13362 13413 13752 13775 13890 14622
14945 15610 16055 16220
16220 16414 17430 18195 18575 19295 19755 20240 20350 20675 22885
```

Stacje numeryczne wzbudzają zainteresowanie radioamatorów. Oni to jako pierwsi wpadli na trop stacji numerycznej, której audycje zaczynały się od hiszpańskiego słowa ¡*Atención*! (uwaga!) (Mason, 1991). Krótkofalowcy odkryli, że jedna z audycji ¡*Atención*! została nadana na częstotliwości należącej do Radia Habana Cuba (Poundstone, 1985), co zostało oficjalnie potwierdzone przez Stany Zjednoczone w roku 2000, gdy amerykańskie źródła rządowe podały do publicznej wiadomości niektóre z odcyfrowanych przekazów (za: Sokol, 2001):

- Życzenia dla wszystkich towarzyszek z okazji 8 marca, czyli Międzynarodowego Dnia Kobiet;
- Ustawić jako priorytet i kontynuować przyjaźń z Joe i Dennisem;
- Agentom German i Caster pod żadnym pozorem nie wolno lecieć BTTR lub inną organizacją w dni 24, 25, 26 i 27.

Do tej pory zanotowano tylko jeden przypadek procesu sądowego zakończonego wyrokiem sądowym za nadawanie audycji numerycznych: Kendall i Gwendolyne Myers zostali o szpiegostwo na rzecz Kuby. Akt oskarżenia zarzucał Kendallowi Myersowi m.in. „nadawanie zaszyfrowanych informacji w paśmie fal krótkich (...) za pośrednictwem alfabetu Morse'a lub czytanych głosem serii cyfr" (United States v. Walter Kendall Myers).

3

Kryptografia asymetryczna i hybrydowa

Cel

Rys historyczny. Omówienie podstawowych pojęć oraz technik kryptografii asymetrycznej. Omówienie i analiza ogólnych problemów związanych z kryptografią asymetryczną.

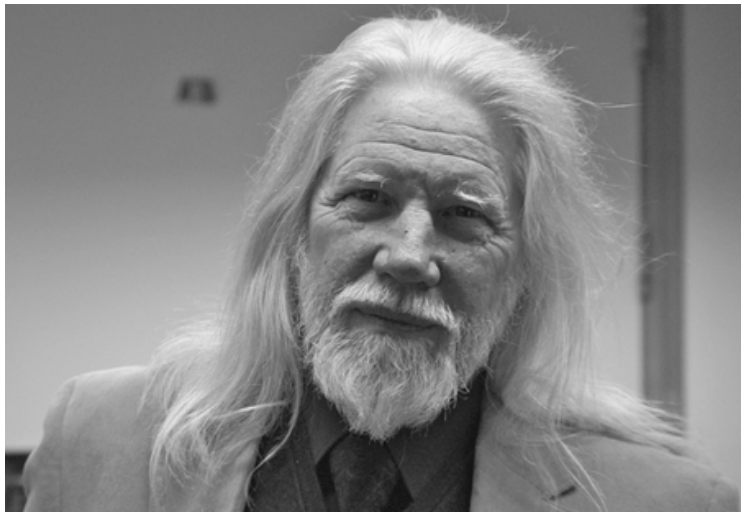
Plan

1. Rys historyczny
2. Kryptografia asymetryczna – pojęcia i definicje
3. Protokół uzgadniania kluczy Diffiego-Hellmana
4. Kryptografia hybrydowa

3.1 RYS HISTORYCZNY

Praktycznie od końca II wojny światowej aż do początku lat siedemdziesiątych XX wieku temat kryptografii był traktowany w zjawisku historycznym, a wszelkie odkrycia w tej dziedzinie nie opuszczały tajnych, dobrze strzeżonych budynków rządowych. W USA organizacją tego typu była National Security Agency, o której mówiono wtedy No Such Agency, ze względu na jej tajność (Singh, 2003).

Jeśli w tamtych czasach kogoś interesował temat kryptografii, to miał on dostęp do nielicznych artykułów i kilku książek. Jednym z takich zapaleńców okazał się urodzony w 1944 roku Amerykanin Bailey Whitfield Diffie (Fot. 3.1), który z kryptografią zetknął się jeszcze w szkole. Jako student matematyki na Massachusetts Institute of Technology (MIT) zajmował się m.in. problemem ochrony danych w sieci, twierdząc, że w dobie rozwoju informatyki i sieci komputerowych nowoczesna technologia powinna chronić dane użytkowników (Kahn, The Codebreakers, 1997).



Fot.3.1. Bailey Whitfield Diffie
(źródło: futurezone.at, 2012)

Po ukończeniu studiów pracował w firmie Mitre. W 1969 roku porzucił pracę i rozpoczął podróż po amerykańskich kampusach uniwersyteckich, gdzie spotykał się z wieloma specjalistami zarówno z dziedziny matematyki, jak i informatyki (Kahn, The Codebreakers, 1997).

Jego marzeniem było opracowanie ogólnodostępnej techniki szyfrowania, której próby złamania powinny okazać się bezcelowe i która umożliwiałaby kontakty dwóm osobom, które wcześniej się nie spotkały i nie mogły wymienić ze sobą kluczy.

Około 1970 roku Diffie poznał Marty'ego Hellmana (Fot. 3.2), doktora Uniwersytetu Stanford, byłego pracownika firmy IBM, późniejszego pracownika Massachusetts Institute of Technology (Kahn, The Codebreakers, 1997).

Jako naukowiec zajmujący się oficjalnie tematyką kryptografii Hellman wielokrotnie był odwiedzany przez pracowników NSA, którzy twierdzili, że zajmując się kryptografią traci tylko czas. Cechy charakterów obu panów sprawiły, że zajęli się oni opracowywaniem pomysłu na nowy rodzaj klucza i kwestionując utarte zasady szyfrowania i deszyfrowania szukali nowych rozwiązań rozpatrując między innymi zastosowanie funkcji jednokierunkowych (vide Rozdział 3.2.1).

Fot.3.2. Martin Hellman
(źródło: Blackman, 2009)

W marcu 1975 roku amerykańskie Narodowe Biuro Normalizacji (National Bureau of Standards – NBS) wydało dokument z propozycją nowego, silnego (jak na tamte czasy) algorytm szyfrowania, który miał nosić nazwę Data Encryption Standard (DES). Był to ruch ze strony władz federalnych na głosy ze środowisk naukowych i sektora prywatnego o wprowadzenie pewnych norm w dziedzinie szyfrowania - vide Rozdział 2.5.1 (Pieprzyk, Hardjono & Seberry, 2006).

Pierwsze analizy jakie wykonali Diffie i Hellman wykazały, że prawdopodobnie w ustalaniu normy długości klucza brali udział pracownicy NSA. Klucz miał bowiem długość 56 bitów, co dawało około 70 tysięcy bilionów możliwych kombinacji. Ilość taka nie stanowiła jednak problemu dla organizacji dysponujących wieloma wysokiej klasy komputerami do przeprowadzenia ataku typu *brute force* w celu odczytania informacji. Uwagi duetu ze Stanford dotyczące DES nie zmieniły zdania władz federalnych o wielkości klucza, zainspirowały jednak do dalszych poszukiwań.

Wszystko zaczęło się jednak kilka lat wcześniej w firmie IBM. Jeden z jej pracowników, Horst Feistel, z pochodzenia Niemiec, jeden z twórców systemu identyfikacji swój-obcy, kryptograf, zaczął już przed rokiem 1973, opracowywać system szyfrowania, który miał zapewnić ochronę prywatności obywatelom (vide Rozdział 2.5.1).

System został nazwany *Demon* od słowa *demonstration*. Później nazwa została zmieniona na *Lucifer* od słowa *cipher* (ang. szyfr). Siła systemu polegała na braku występowania charakterystycznych wzorów przez poddanie znaków tekstu jawnego zawiłym zabiegom matematycznym polegających na wielokrotnych podstawieniach. Zaszyfrowany tekst miał formę bloku przypadkowo dobranych liter. Feistel utworzył kilka wersji szyfru, a najbardziej popularna opierała się na studwudziesto-ośmiobitowym kluczu (Singh, 2003).

IBM zauważyło możliwość zastosowania Lucyfera w bankowości. Wymagało to jednak dopracowania systemu, który poza niezawodnością techniki szyfrowania musiał być tani w implementacji i użytkowaniu oraz działać bardzo szybko.

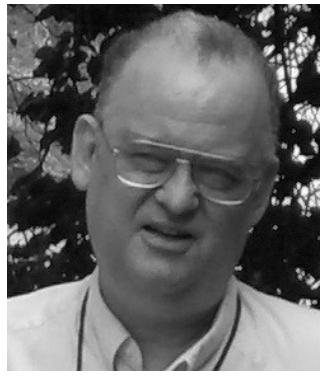
Udoskonalona wersja Lucyfera nosiła miano DSD-1. Dysponował on ośmioma, a nie jak poprzednik dwoma tzw. S-blokami i mógł pobierać bloki tekstu jawnego liczące 64 bity (Singh, 2003).

Aby Lucifer mógł stać się normą, IBM była zmuszona do opublikowania części materiałów dotyczących tego szyfru. Ich materiałów zbiegło się z wezwaniem przedstawicieli IBM do siedziby NSA. Agencja zaproponowała, że dokona testów układu i będzie pomagać w usuwaniu błędów, jeśli tylko IBM zechce utrzymać wszystko w tajemnicy, będzie rozprzestrzeniał jedynie układy wykorzystujące szyfr, a nie algorytmy i nie będzie wysyłał układów do państw, z którymi agencja wcześniej nie podpisze odpowiednich zobowiązań (Kahn, The Codebreakers, 1997). IBM przystała na umowę z NSA (Singh, 2003). Pracownicy firmy związani z projektem otrzymali zakaz wypowiadania się na temat DSD-1, a wszelkie informacje dotyczące projektu zostały opatrzone pieczątkami "ściśle tajne" (Singh, 2003). Współpraca okazała się owocna, ponieważ specjaliści NSA wykryli wiele specyficznych sytuacji, gdy kod mógł zostać złamany (Singh, 2003). Ostatecznie DSD-1 utracił 128 bitowy klucz na rzecz 56 bitowego, który stał się normą w DES. IBM nie mogło się nie zgodzić ze zmianami, aby nie utracić możliwości sprzedaży układu za granicą, a klucz 56 bitowy był mimo wszystko ówcześnie uważany za dostatecznie silny (Singh, 2003).

Również na początku roku 1975 Diffie i Hellman zorganizowali nieformalne seminarium na temat kryptografii. Jednym z zaproszonych gości był informatyk z Berkley, Peter Blatman. Dzięki niemu duet poszukiwaczy nowego systemu dowiedział się, że jeden z przyjaciół gościa, Ralph Merkle (Fot. 3.3.) zajmuje się tematem prowadzenia bezpiecznej konwersacji na linii pozbawionej zabezpieczeń w sytuacji, gdy uczestnicy nie znali się wcześniej i nie mogli wymienić między sobą kluczy (Singh, 2003).

Diffie opierając się na swoich dotychczasowych doświadczeniach stwierdził, że jest to niemożliwe, ale jeszcze w maju tego samego roku odkrył sposób na rozwiązanie tego problemu. Stwierdził, że klucz należy **podzielić**.

To przełomowe rozwiązanie było istną herezją w dotychczasowej historii kryptografii. Rozwiązywało ono jednak **problem nieuczciwego administratora** (który mógł skopiować klucz przed wydaniem go którejś ze stron transmisji), jednocześnie usuwając problemy, jakie mogłyby wyniknąć w trakcie przekazywania kluczy tajnych pomiędzy obywatelami (tj. problem biurokratyzacji, opóźnień i możliwości zdobycia kluczy poprzez łapówki, włamania itp.).



Fot.3.3. Ralph C. Merkle
(źródło: Wikimedia Commons)

W przypadku systemu Diffiego, każda osoba mogła generować unikatową parę kluczy na własną rękę. Para taka miała składać się z **klucza publicznego** i **prywatnego**. Diffie chciał tu wykorzystać **funkcje jednokierunkowe**, co dawało gwarancję, że poznanie klucza prywatnego, którym zaszyfrowano wiadomość nie wiązało się z ryzykiem jej odszyfrowania (Singh, 2003).
Wiadomość taka mogła być odczytana przez prawowitego odbiorcę przy użyciu jego osobistego klucza prywatnego. Taka technika zapewniała autentyczność dokumentu, a zastosowanie klucza prywatnego było niemal równoznaczne z osobistym złożeniem podpisu pod wysyłanym dokumentem (Levy, 2001).

Na początku lutego 1976 roku doktor Hellman otrzymał list od Ralpha C. Merkle zawierający jego pracę dotyczącą podobnej koncepcji, jak teoria Diffiego. Merkle zaproponował współpracę, która została przyjęta, gdy w maju 1976 roku Hellman w trakcie prac nad potęgowaniem dyskretnym opracował odpowiedni algorytm, nazywany później algorytmem Diffiego-Hellmana. Hellman zaprosił Merkle do współpracy jako badacza na okres wakacji. Współpraca okazała się na tyle owocna, że jeszcze w listopadzie 1976 roku ukazała się praca Diffiego i Hellmana, pod tytułem *New Directions in Cryptography*, ukazująca nie tylko problemu klasycznej wówczas kryptografii w zasięgu globalnym, ale także jak je rozwiązać (Diffie & Hellman, 1976).

Fot.3.4. Od lewej: Ralph C. Merkle, Martin Hellman, Bailey Whitfield Diffie w trakcie prac nad ideą kryptografii asymetrycznej (źródło: C.Painter, Stanford News Service)

Wśród czytelników tego artykułu był Ron Rivest (Fot. 3.5), docent na Massachusetts Institute of Technology. Zajął się on pracami nad algorytmem bazującym na pomyśle Diffiego i Hellmana. W niedługim czasie dołączył do niego Leonard Adleman (Fot. 3.5), teoretyk matematyki, a potem także matematyk izraelskiego pochodzenia, nowy członek wydziału komputerowego MIT, Adi Shamir (Fot. 3.5).

Przez niemal pół roku testowali różne, wymyślane przez siebie systemy (Levy, 2001).

W kwietniu 1977 Rivest wymyślił system oparty na teorii liczb i rozkładaniu na czynniki pierwsze. Nie był to pierwszy pomysł tego typu, ale ten był ściśle dopracowany i uproszczony, a co istotne spełniał wszelkie założenia opracowane przez Diffiego i Hellmana (Levy, 2001). System ten został nazwany RSA (od nazwisk współpracowników – Rivesta, Shamira i Adlemana).

Fot.3.5. Od lewej: Ron Rivest, Adi Shamir i Leonard Adleman w 2003 (źródło: usc.edu, 2003)

Dla NSA rozpoczął się okres, który można śmiało nazwać horrorem. Złożyły się na to nie tylko opisane powyżej odkrycia, ale także kontrole związane z częstymi praktykami podsłuchiwania oraz innymi przekroczeniami norm prawnych.
Już w 1975 roku NSA zaczęło starać się o ograniczenie swobód obywatelskich w dziedzinie kryptografii (Levy, 2001).

Jednym z pierwszych działań było ogłoszenie, że jedynie NSA może finansować prace związane z kryptografią. Oznaczało to, że wszyscy pracownicy uniwersytetów, którzy zajmują się innowacjami w tej dziedzinie działają poza prawem.
Na szczęście dla środowiska kryptologów działanie to zakończyło się porażką, ponieważ nie istniał żaden akt prawny potwierdzający takie stanowisko (Levy, 2001).

Podejmowane przez NSA działania zwróciły jednak uwagę twórców RSA na problem wysyłania materiałów za granicę. Władze MIT radziły, aby powstrzymać się przed tym aż do czasu oficjalnego wyjaśnienia sprawy (Levy, 2001). Ponieważ NSA przez około pół roku nie była wstanie dać konkretnej odpowiedzi, zaś prawnicy ze Stanford (którzy zajmowali się problemem na prośbę Hellmana) i Massachusetts zgodnie stwierdzili, że powszechna publikacja wyników jest zgodna z prawem, RSA zostało zgłoszone do opatentowania w grudniu 1977 roku (Levy, 2001). Patent ten wygasał 21 września 2000, jednak zdecydowano się na przekazanie systemu do domeny publicznej dwa tygodnie wcześniej, 6 września.

Następnym przedsięwzięciem trójki ambitnych naukowców było założenie własnej firmy, zajmującej się komercyjnym wykorzystaniem kryptografii. Pierwsze próby zakończyły się porażką i niemal bankructwem firmy RSA. Przełom nastąpił dopiero w 1984 roku za sprawą programu Notes firmy LOTUS, która w sposób komercyjny, wykorzystywała algorytm autorstwa Rivesta, Shamira i Adlemana (Levy, 2001).

Na początku lat 90-ych NSA musiała stawić czoła kolejnemu problemowi – Philowi Zimmermannowi (Fot. 3.6) i jego programowi znanemu dzisiaj pod nazwą Pretty Good Privacy (PGP).

Fot.3.6. Phil Zimmerman
(źródło: Wikimedia Commons)

Program ten gwarantował szyfrowanie o wysokim stopniu skuteczności za pomocą kluczy asymetrycznych (czyli opartych na pomyśle Diffiego).
NSA nie chciało wydać zgody na eksport programu zasłaniając się bezpieczeństwem publicznym (Levy, 2001). Skazywało to projekt PGP na klęskę zarówno pod względem komercyjnym jak i ideowym. Rozwiązanie tej historii przypomina fragment filmu sensacyjnego – Zimmermann wraz ze wspólnikami wydrukował kod źródłowy programu w kilku kopiach wywiózł za granicę (Levy, 2001).

Walizki zawierające po kilka tysięcy stron wydruku przekazał w ręce zaufanych współpracowników, którzy będąc poza granicami USA mogli bez przeszkód rozpowszechnić program w wersji elektronicznej (Levy, 2001). Zakaz NSA stał się rzeczą absurdalną, bowiem PGP było dostępne na całym świecie.

Rozpoczęła się nowa era kryptografii.

3.2 KRYPTOGRAFIA ASYMETRYCZNA – POJĘCIA I DEFINICJE

Kryptografia asymetryczna to rodzaj kryptografii, w którym używa się zestawów dwu (najczęściej) lub więcej powiązanych ze sobą kluczy, umożliwiających wykonywanie różnych czynności kryptograficznych.

Kryptografia asymetryczna została oficjalnie wynaleziona przez cywilnych badaczy Martina Hellmana, Whitfielda Diffie i niezależnie przez Ralpha Merkle w 1976 roku. Dopiero pod koniec XX wieku brytyjska służba wywiadu elektronicznego GCHQ ujawniła, że pierwsza koncepcja systemu szyfrowania z kluczem publicznym została opracowana przez jej pracownika Jamesa H. Ellisa już w 1965 roku, a działający system stworzył w 1973 roku Clifford Cocks, również pracownik GCHQ.
Odkrycia te były jednak objęte klauzulą tajności do 1997 roku (Singh, 2003).

Ponieważ kryptografia asymetryczna jest o wiele wolniejsza od symetrycznej, w zastosowaniach cywilnych prawie nigdy nie szyfruje się całości wiadomości za jej pomocą – zamiast tego szyfrowany jest jedynie klucz jakiegoś szyfru symetrycznego (Bishop, 2004).

3.2.1 FUNKCJE JEDNOKIERUNKOWE

Algorytmy mające zastosowanie w kryptografii asymetrycznej wykorzystują funkcje jednokierunkowe – czyli takie, które są relatywnie proste do obliczenia, zaś ich wyniki są relatywnie trudne do odwrócenia (Garbarczuk & Świć, 2005).

Prosta do obliczenia oznacza, że istnieje obliczający ją algorytm wielomianowy. **Trudna do odwrócenia** oznacza, że żaden wielomianowy algorytm probabilistyczny nie potrafi znaleźć elementu przeciwobrazu *f(x)* z prawdopodobieństwem większym niż zaniedbywalne, jeśli x jest wybrane losowo.

Istnienie funkcji jednokierunkowych jest otwartym problemem w informatyce. Istnienie tych funkcji pozwoliłoby uzyskać wiele przydatnych w kryptografii narzędzi, takich jak chociażby (za: Schneier, 2002):

- generatory liczb pseudolosowych;
- protokoły zobowiązania bitowego;
- bezpieczne kody uwierzytelniające wiadomości;
- bezpieczne podpisy elektroniczne.

Ponieważ do tej pory nie wiadomo, czy funkcje jednokierunkowe istnieją, w praktyce używa się kilku funkcji, które są o to podejrzewane – funkcji, dla których pomimo wysiłku wielu badaczy nie udało się znaleźć efektywnych algorytmów odwracających (Schneier, 2002).

Przykładowo algorytm RSA opiera się na założeniu, że operacja mnożenia jest operacją łatwą, zaś faktoryzacja wyniku (czyli jego rozkład na czynniki) jest operacją trudną. Także w przypadku ElGamal i DSA potęgowanie modulo jest operacją relatywnie prostą obliczeniowo, zaś jej odwrócenie (logarytmowanie dyskretne) jest złożone obliczeniowo.

3.2.2 KLUCZ PRYWATNY I PUBLICZNY

Najważniejsze zastosowania kryptografii asymetrycznej – szyfrowanie i uwierzytelnianie – zakładają istnienie pary kluczy – prywatnego i publicznego, przy czym w niektórych innych zastosowaniach kluczy może być więcej (Diffie

& Hellman, 1976). Klucz prywatny nie jest możliwy do łatwego odtworzenia na podstawie publicznego.

Klucz publiczny używany jest do zaszyfrowania informacji, **klucz prywatny** zaś do jej odczytu. Ponieważ klucz prywatny jest w wyłącznym posiadaniu adresata informacji, tylko on może ją odczytać (Diffie & Hellman, 1976). Natomiast klucz publiczny jest udostępniony każdemu, kto zechce zaszyfrować wiadomość – może być np. udostępniony publicznie na stronie internetowej lub na wizytówce.
We wszystkich kryptosystemach uzyskanie klucza prywatnego na podstawie publicznego musi być obliczeniowo trudne (Garbarczuk & Świć, 2005).

Przykład działania asymetrycznego systemu kryptograficznego opartego o parę kluczy prywatny – publiczny został przedstawiony na rysunku 3.7.

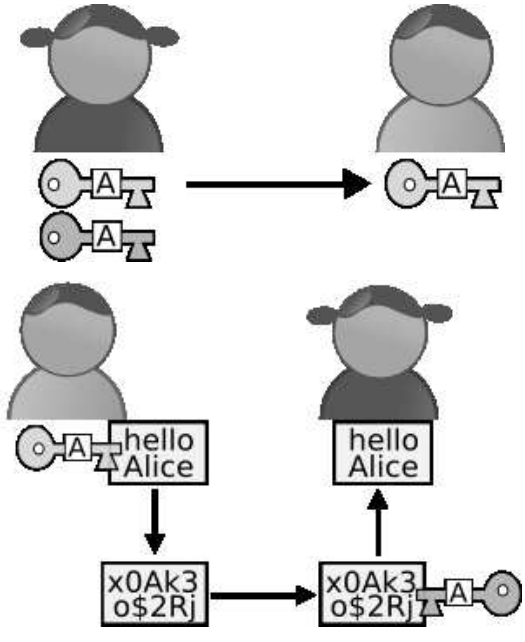
Do opisu użyto przyjętych w kryptografii oznaczeń – nadawca i odbiorca określani są jako Alice i Bob, zaś potencjalny podsłuchujący jako Eve, co jest skrótem od *evesdropper* – co jest angielskim określeniem podsłuchiwacza (Schneier, 2002). W polskich tłumaczeniach, m.in. (Singh, 2003) można spotkać się określaniem stron komunikacji mianem Alicji i Bolka, zaś podsłuchujący nazywany jest Ewą.
Po raz pierwszy te trzy postacie pojawiły się po raz pierwszy w artykule opisującym działania RSA (Rivest, Shamir & Adleman, 1978).

Jako ciekawostkę można podać, że w opisie procesów kryptograficznych wykorzystuje się także inne postacie z predefiniowanymi rolami. Są to m.in. (za: Schneier, 2002):

- Carol, Carlos lub Charlie – trzeci uczestnik konwersacji;
- Chuck – trzeci uczestnik konwersacji, który często ma złośliwe zamiary w stosunku do Alice i Boba (choć nie należy utożsamiać go z Ewą ani z Mallorym);
- Craig – osobnik łamiący hasła (ang. *cracker*);
- Dave albo Dan – czwarty uczestnik;
- Izaak – wystawca dokumentu (ang. *issuer*);
- Justin – wymiar sprawiedliwości (ang. *justice system*);
- Mallory – szkodliwy uczestnik (ang. *malicious attacker*), który – w przeciwieństwie do Ewy – może modyfikować, zamieniać, powtarzać stare przekazy itd. Znacznie

trudniej jest zabezpieczyć system przed Mallorym niż przed Ewą. Zamiennie używane jest również Marvin i Mallet;

- Matilda, kupiec (ang. *merchant*), np. w finansach lub e-commerce;
- Oscar, przeciwnik, często używany zamiennie z Mallorym, choć nie zawsze jego działania muszą być szkodliwe;
- Peggy i Victor weryfikują (ang. *prover* oraz *verifier*), czy dane zdarzenie miało faktycznie miejsce;
- Trent, zaufany sędzia (ang. *trusted arbitrator*), którego dokładna rola zmienia się zależnie od rodzaju omawianego protokołu;
- Walter – strażnik (ang. *warden*), używany czasem w niektórych bezpiecznych systemach;
- Zoe, zazwyczaj ostatnia postać we wszystkich protokołach kryptograficznych.



Rys. 3.7. Krok 1: Bob uzyskuje od Alice jej klucz publiczny. Krok 2: Bob przesyła do Alice wiadomość zaszyfrowaną przy użyciu jej klucza publicznego. Krok 3: Alice odszyfrowuje otrzymaną od Boba wiadomość za pomocą swojego klucza prywatnego
(źródło: Garbarczuk & Świć, 2005)

3.2.3 PROTOKÓŁ UZGADNIANIA KLUCZY DIFFIEGO – HELLMANA

Protokół ten umożliwia dwóm stronom wylosowanie takiej pewnej liczby, znanej – po wykonaniu protokołu – dla obydwu stron, lecz nie dla osoby próbującej podsłuchać wymianę wiadomości. W ten sposób wylosowana liczba może być użyta jako klucz do szyfrowania komunikacji (Diffie & Hellman, 1976).

Protokół nie zabezpiecza przed ingerencjami w komunikację (np. atak typu *man in the middle*), jedynie przed pasywnym podsłuchem. Oznacza to, iż należy go dodatkowo uzupełnić o zabezpieczenia przed atakiem aktywnym (Schneier, 2002).
Schemat działania protokołu przedstawia się następująco (za: Schneier, 2002):

- Alicja i Bob w dowolny sposób wybierają dwie liczby względnie pierwsze: dużą liczbę *p* oraz liczbę *g*, będącą generatorem grupy multiplikatywnej *Zp**;
  Liczby te mogą być opublikowane wcześniej np. na stronie internetowej albo na wizytówce, bądź też uzgodnione online. Zachowanie ich tajności nie jest istotne dla bezpieczeństwa całej procedury;
- Alicja losuje liczbę *a;*
- Bob losuje liczbę *b*;
- Alicja wysyła Bobowi liczbę A, będącą wynikiem równania $A=g^a \bmod p$;
- Bob wysyła Alicji liczbę B, będącą wynikiem równania $B=g^b \bmod p$;
- Alicja oblicza $K=(g^b)^a \bmod p = g^{ab} \bmod p$;
- Bob oblicza $K=(g^a)^b \bmod p = g^{ab} \bmod p$;
- Podsłuchujący (Eve) zna g, A i B, jednak bez obliczenia logarytmu dyskretnego nie jest w stanie obliczyć K;
- Wynikowo, Alicja nie zna liczby b wylosowanej przez Boba, zaś Bob nie zna liczby a wylosowanej przez Alicję.

3.3 WYBRANE ALGORYTMY KRYPTOGRAFII ASYMETRYCZNEJ

3.3.1 RSA

RSA opiera się na trudności faktoryzacji dużych liczb (Rivest, Shamir & Adleman, 1978) – znalezienie szybkiej metody faktoryzacji doprowadziłoby do złamania tego algorytmu (Schneier, 2002).

W literaturze (m.in. (Merike, 2000; Bishop, 2004) nie znaleziono jednak dowodu na to, że RSA nie jest możliwe do złamania w inny sposób.

W celu wygenerowania klucza RSA losowane są dwie duże liczby pierwsze *p* i *q*, a także liczba względnie pierwsza *e*, równa

$$e=(p-1)(q-1)$$

Liczby względnie pierwsze to takie liczby całkowite, które w rozkładzie na czynniki pierwsze nie mają wspólnych dzielników poza jedynką.

Następnie obliczana jest liczba *d*:

$$d=e^{-1} \bmod (p-1)(q-1)$$

Ponieważ e jest liczbą względnie pierwszą, to ma ona odwrotność, która można obliczyć relatywnie szybko za pomocą rozszerzonego algorytmu Euklidesa.

Obliczana jest również liczba *n*:

$$n=p*q$$

Kluczem publicznym jest para liczb (*e,n*), zaś kluczem prywatnym jest para liczba (*d,n*). Algorytm RSA zakłada zniszczenie liczb *p* i *q*.

Aby zaszyfrować wiadomość, należy podnieść reprezentującą ją liczbę (wartość bitową) do potęgi *e* i dokonać dzielenia modulo *n*.

Stosując oznaczenia z rozdziału 2 operację tą można zapisać w postaci wzoru:

$$C=P^e \bmod n$$

Aby odszyfrować szyfrogram, należy podnieść zaszyfrowaną wiadomość do potęgi *d* – zgodnie z twierdzeniem Eulera :

$$C^d = P^{ed} = P \bmod n$$

Odszyfrowanie wiadomości bez znajomości *d* jest trudne obliczeniowo.

Obecnie nie istnieje łatwa obliczeniowo metoda odtworzenia liczby *d* z *e* bez faktoryzacji *n* na *p* i *q*.

3.3.2 ELGAMAL

ElGamal jest algorytmem kryptografii asymetrycznej opartym na trudności problemu logarytmu dyskretnego w ciele liczb całkowitych przy dzieleniu modulo przez dużą liczbę pierwszą (Schneier, 2002).

Generacja klucza odbywa się w następujący sposób (za: Schneier, 2002):
wybierana jest dowolna liczba pierwsza p, dowolny generator a podgrupy multiplikatywnej (czyli taki element, którego rząd jest równy p) oraz dowolne k spełniające warunek $1<k<p$.
Następnie obliczane jest b takie, że:

$$b=a^k$$

Rolę klucza publicznego pełnią liczby (p,a,b), zaś rolę klucza prywatnego – k.

Aby zaszyfrować wiadomość za pomocą ElGamal reprezentację liczbową wiadomości P przedstawia się jako element grupy $[1<P<p-1]$, następnie wybierana jest liczba y należąca do zbioru $\{2,(p-1)\}$. Kolejnym krokiem jest obliczenie c_1 i c_2 podług poniższych wzorów:

$$c_1=a^y$$

$$c_2=Pb^y$$

Para liczb (c_1,c_2) stanowi szyfrogram wiadomości.

Aby odszyfrować wiadomość, należy najpierw obliczyć liczbę d podług wzoru:

$$d=c_1^k$$

zaś następnie można już obliczyć tekst jawny P, jako

$$P=c_2/d$$

Jeżeli rząd grupy multiplikatywnej (p) nie jest iloczynem dużych liczb pierwszych, to istnieje wtedy efektywna metoda obliczania wykładnika – jest to tak zwana redukcja Pohliga-Hellmana (Schneier, 2002).
Obecnie nie jest znana „ogólna” metoda relatywnie szybkiego obliczenia logarytmu dyskretnego, więc nie istnieje możliwość określenia k za pomocą a i c_1.

3.3.3 FUNKCJE SKRÓTU ORAZ DSA

Funkcja skrótu (często określana też mianem funkcji haszującej) to funkcja, która przyporządkowuje dowolnie dużej liczbie (wiadomości) krótką, zwykle posiadającą stały rozmiar wartość (skrót tej wiadomości) (Garbarczuk & Świć, 2005).

W informatyce funkcje skrótu pozwalają na ustalenie krótkich i łatwych do weryfikacji sygnatur dla dowolnie dużych zbiorów danych. Ich zadaniem jest ochrona przed przypadkowymi lub celowo wprowadzonymi modyfikacjami danych, są również stosowane przy optymalizacji dostępu do struktur danych w programach komputerowych (Schneier, 2002). Szczególną podgrupą funkcji skrótu są funkcje uznawane za bezpieczne do zastosowań kryptograficznych.

Powinny one spełniać następujące kryteria (za: Schneier, 2002):

- brak praktycznej możliwości wygenerowania wiadomości o takim samym skrócie jak zadana wiadomość (tzw. kolizji)
- brak praktycznej możliwości wygenerowanie dwóch wiadomości o takim samym skrócie. Własność ta nie jest wymagana w niektórych zastosowaniach
- brak możliwości wnioskowania o wiadomości wejściowej na podstawie wartości skrótu.

W szczególności oznacza to, że zmiana nawet jednego bitu wiadomości powinna zmieniać średnio połowę bitów skrótu (Schneier, 2002).

Należy zauważyć, że uznanie funkcji za bezpieczną do zastosowań kryptograficznych opiera się zawsze wyłącznie na domniemanej odporności na znane ataki kryptoanalityczne, nie zaś na matematycznych dowodach gwarantujących niemożność złamania. Bezpieczna funkcja skrótu musiałaby być funkcją jednokierunkową, a istnienie takich funkcji nie zostało dotychczas dowiedzione.

Najczęściej stosowanym algorytmem asymetrycznym wykorzystującym funkcję skrótu (konkretnie jest to SHA-1) jest Digital Signature Algorithm (DSA), stosowany jako amerykański narodowy standard dla podpisów cyfrowych (Schneier, 2002). Używa on kluczy o długości od 512 do 1024 bitów, adekwatnie do aktualnych mocy obliczeniowych.

Aktualnie DSA używane jest w OpenSSL, OpenSSH i GnuPG (vide Roz. 3.5.), gdzie standardowo używane są klucze o długości przynajmniej 768 bitów.

3.4 KRYPTOGRAFIA HYBRYDOWA

Szyfrowanie asymetryczne uznawane jest aktualnie za najsilniejszą z metod kryptologicznych dostępnych do zastosowań cywilnych. Jednak jego główną wadą pozostaje fakt, iż algorytmy asymetryczne są o wiele wolniejsze od symetrycznych. Może to powodować znaczące utrudnienia w wykorzystywaniu ich do szyfrowania dużych ilości danych, szczególnie za pomocą silnych kluczy (Schneier, 2002).

Idealnym rozwiązaniem wydaje się więc użycie kryptografii hybrydowej, która prawdopodobnie została zastosowana po raz pierwszy do celów cywilnych w PGP. Opiera się ona o następujące założenia (za: Schneier, 2002):

- dane szyfrowane są przy użyciu szybkiego szyfru symetrycznego (np. 3DES czy AES) za pomocą całkowicie losowo wygenerowanego klucza;
- klucz użyty do zaszyfrowania wiadomości jest następnie zaszyfrowywany szyfrem asymetrycznym (np. RSA) i jest dołączany do przesyłanej wiadomości.

Aby odszyfrować wiadomość, odbiorca musi najpierw odszyfrować klucz, a następnie użyć go do odszyfrowania właściwej wiadomości.

Jak łatwo więc zauważyć, użycie kryptografii hybrydowej umożliwia relatywnie szybkie zaszyfrowanie dużej ilości danych przy jednoczesnym bezpiecznym przesyle klucza szyfrującego do odbiorcy.

3.5 TECHNIKI WYKORZYSTUJĄCE KRYPTOGRAFIĘ ASYMETRYCZNĄ BĄDŹ HYBRYDOWĄ

3.5.1 TLS / SSL

W 1994 roku firma Netscape stworzyła protokół służący do bezpiecznej transmisji zaszyfrowanego strumienia danych, który nazwano SSL (Secure Socket Layer) (Rescorla, 2001).

Jego pierwsza wersja miała jednak poważną dziurę w bezpieczeństwie, gdyż procedury uzgadniania szyfru nie były zabezpieczone, więc atakujący mógł

wymusić używanie najsłabszego szyfru obsługiwanego przez komunikujących się, ze złamaniem którego mógł sobie poradzić znacznie łatwiej niż z szyfrem, który strony wybrałyby normalnie (Rescorla, 2001). W 1996 roku Internet Engineering Task Force powołało grupę roboczą pod nazwą Transport Layer Security, której zadaniem było rozwijanie protokołu SSL (Rescorla, 2001).

W 1999 roku został opublikowany standard TLS 1.0, który jest czasem określany jako SSL 3.1 (Schneier, 2002). Całość działa w architekturze klient-serwer, pozwalając na nawiązanie bezpiecznego połączenia z użyciem certyfikatów. Architektura jest zorientowana głównie na uwierzytelnianie serwera (np. sklepu internetowego, do którego klient wysyła numer karty kredytowej i chce mieć pewność co do odbiorcy), ale przewiduje również możliwość uwierzytelniania klienta.

Krytycznym parametrem określającym siłę szyfrowania SSL jest długość użytych kluczy (Rescorla, 2001). Im dłuższy klucz, tym trudniej jest go złamać, a przez to odszyfrować transmisję. Dla kluczy asymetrycznych, zgodnie z zaleceniami NIST, długością sugerowaną jest obecnie 2048 bitów. Powszechnie używane wyrażenia „SSL 128 bitów" oraz „SSL 40 bitów" określają długość użytego klucza symetrycznego (Rescorla, 2001).

Z powodu ograniczeń w eksporcie technologii kryptograficznych ze Stanów Zjednoczonych, większość implementacji protokołu SSL nie mogła wykorzystywać kluczy symetrycznych dłuższych niż 40 bitów (Levy, 2001). Dzięki temu rządowe agencje bezpieczeństwa dysponujące odpowiednio dużą mocą obliczeniową (m.in. NSA) były w stanie złamać szyfr metodą brute-force. Po kilku latach publicznej debaty, lepszemu poznaniu dłuższych kluczy przez zainteresowane strony oraz kilku sprawach sądowych, amerykański rząd złagodził swoje stanowisko wobec stosowania większych kluczy. Obecnie 40-bitowe klucze wyszły z użycia i zostały zastąpione przez zapewniające większe bezpieczeństwo klucze o długości 128 i więcej bitów (Levy, 2001).

Zarówno SSL i TLS to ustandaryzowane zestawy wcześniej znanych algorytmów, technik i schematów używanych do zapewnienia bezpieczeństwa. Wykorzystują algorytmy szyfrowania (za: Schneier, 2002):

- symetryczne – do szyfrowania i deszyfrowania danych używany jest ten sam klucz, tak więc znając klucz szyfrujący można dokonać również deszyfracji danych (wyznaczyć klucz deszyfrujący);
- asymetryczne (z kluczem publicznym) – do szyfrowania i deszyfrowania używane są różne klucze, tak więc znając klucz szyfrujący nie możemy odszyfrować wiadomości (klucza deszyfrującego nie da się w prosty sposób wyznaczyć z klucza szyfrującego); klucz służący do szyfrowania jest udostępniany publicznie (klucz publiczny), ale informację nim zakodowaną może odczytać jedynie posiadacz klucza deszyfrującego (klucz prywatny), który nie jest nikomu ujawniany.

SSL jest najczęściej kojarzony z protokołem HTTP (HTTPS), ale może służyć do zabezpieczania wielu innych protokołów, m.in.: Telnet, SMTP, POP, IMAP czy FTP, gdyż protokoły te same w sobie nie zapewniają szyfrowania transmisji.

W kodowanym kanale transmisji SSL może być przenoszonych wiele sesji HTTP. Dane podczas transmisji są szyfrowane kluczem symetrycznym, jednak na początku sesji sam klucz symetryczny jest przesyłany przy wykorzystaniu algorytmu niesymetrycznego (RSA, Diffiego-Helmana). Integralność zapewniają podpisy elektroniczne.

Zasada działania

Schemat działania protokołu wygląda następująco (za: Rescorla, 2001), przy czym K oznacza klienta, zaś S – serwer:

1. K → S ClientHello

Klient wysyła do serwera zgłoszenie zawierające m.in. obsługiwaną wersję protokołu SSL, dozwolone sposoby szyfrowania i kompresji danych oraz identyfikator sesji. Komunikat ten zawiera również losową liczbę, która jest potem używana przy generowaniu kluczy.

2. K ← S ServerHello

Serwer odpowiada podobnym komunikatem w którym zwraca klientowi wybrane parametry połączenia: wersję protokołu SSL, rodzaj szyfrowania i kompresji, oraz podobną liczbę losową.

3. K ← S Certificate

Serwer wysyła swój certyfikat pozwalając klientowi na sprawdzenie swojej tożsamości (ten etap jest opcjonalny, ale występuje w większości przypadków).

4. K ← S ServerKeyExchange

Serwer wysyła informację o swoim kluczu publicznym. Rodzaj i długość tego klucza jest określony przez typ algorytmu przesłany w poprzednim komunikacie.

5. K ← S ServerHelloDone

Serwer zawiadamia, że klient może przejść do następnej fazy zestawiania połączenia.

6. K → S ClientKeyExchange

Klient wysyła serwerowi wstępny klucz sesji, zaszyfrowany za pomocą klucza publicznego serwera. Na podstawie ustalonych w poprzednich komunikatach dwóch liczb losowych (klienta i serwera) oraz ustalonego przez klienta wstępnego klucza sesji obie strony generują klucz sesji używany do faktycznej wymiany danych. Wygenerowany klucz jest kluczem algorytmu symetrycznego (zazwyczaj jest to DES). Jest on jednak ustalony w sposób bezpieczny i znany jest tylko komunikującym się stronom.

7. K → S ChangeCipherSpec

Klient zawiadamia, że serwer może przełączyć się na komunikację szyfrowaną.

8. K → S Finished

... oraz że jest gotowy do odbierania danych zakodowanych.

9. K ← S ChangeCipherSpec

Serwer zawiadamia, że wykonał polecenie – od tej pory wysyłał będzie tylko zaszyfrowane informacje...

10. K ← S Finished

...i od razu wypróbowuje mechanizm – ten komunikat jest już wysyłany bezpiecznym kanałem.

Uwierzytelnianie klienta

W protokole SSL domyślna sytuacja zakłada tylko uwierzytelnianie serwera. Istnieją jednak metody pozwalające na uwierzytelnienie klienta. W tym celu korzysta się z trzech dodatkowych komunikatów (za: Rescorla, 2001):

1. K ← S CertificateRequest

Po przesłaniu swojego certyfikatu serwer zawiadamia, że chciałby otrzymać certyfikat klienta.

2. K → S Certificate

Po otrzymaniu komunikatu ServerHelloDone klient odsyła swój certyfikat.

3. K → S CertificateVerify

Klient musi potwierdzić, że faktycznie posiada klucz prywatny odpowiadający wysłanemu certyfikatowi. W tym celu klient podpisuje swoim kluczem prywatnym skrót wszystkich dotychczas ustalonych danych o połączeniu i wysyła go korzystając z tego komunikatu.

Odtwarzanie poprzedniej sesji

Nawiązanie połączenia SSL jest procesem dość długotrwałym i wymagającym skomplikowanych obliczeń. W przypadku wielu krótkich połączeń pożądana byłaby możliwość kontynuowania połączenia bez ponownej wymiany kluczy publicznych, ustalania klucza sesji itp.

Protokół SSL przewiduje taką możliwość. Jeżeli w komunikacie ClientHello klient poda SessionId równy identyfikatorowi jednej z poprzednich sesji, to serwer przyjmie, że klient chce kontynuować połączenie z użyciem poprzednio używanego klucza (Rescorla, 2001).

3.5.2 SSH

SSH to standard protokołów komunikacyjnych używanych w sieciach komputerowych TCP/IP, w architekturze klient-serwer (Schneier, 2002).

W ścisłym znaczeniu SSH to tylko następca protokołu Telnet, służącego do terminalowego łączenia się ze zdalnymi komputerami. SSH różni się od Telnetu tym, że transfer wszelkich danych jest zaszyfrowany oraz możliwe jest rozpoznawanie użytkownika na wiele różnych sposobów (Starościak, 2004).

W szerszym znaczeniu SSH to wspólna nazwa dla całej rodziny protokołów, nie tylko terminalowych, lecz także służących do przesyłania plików (SCP, SFTP), zdalnej kontroli zasobów, tunelowania i wielu innych zastosowań. Wspólną cechą

wszystkich tych protokołów jest identyczna z SSH technika szyfrowania danych i rozpoznawania użytkownika (Starościak, 2004).

Obecnie protokoły z rodziny SSH praktycznie wyparły wszystkie inne mniej bezpieczne protokoły, takie, jak np. rlogin czy RSH.

Ogólne założenia protokołu SSH powstały w grupie roboczej IETF. W użyciu są obie jego wersje – 1 i 2. W wersji 2 możliwe jest użycie dowolnych sposobów szyfrowania danych i 4 różnych sposobów uwierzytelnienia, podczas gdy SSH1 obsługiwało tylko stałą listę kilku sposobów szyfrowania i 2 sposoby rozpoznawania użytkownika (klucz RSA i zwykłe hasło) (Stallings, 1997). Najczęściej stosowany sposób szyfrowania to AES, choć część serwerów nadal używa szyfrowania Blowfish i technik z rodziny DES. Uwierzytelnienie użytkownika może się opierać na haśle, kluczu (RSA, DSA) lub protokole Kerberos (Schneier, 2002).

3.5.3 IPSEC

Protokoły wchodzące w skład architektury IPsec służą do bezpiecznego przesyłania przez sieć pakietów IP. Działają one na zasadzie enkapsulacji. Oznacza to, że oryginalny (zabezpieczany) pakiet IP jest szyfrowany, otrzymuje nowy nagłówek protokołu IPsec i w takiej formie jest przesyłany przez sieć (Paterson & Yau, 2006).
Bezpieczeństwo zapewniane przez IPsec może być dwojakie, w zależności od stosowanego protokołu. Do celów dystrybucji klucza i uwierzytelniania stron stworzono oddzielny protokół IKE (Paterson & Yau, 2006).

Protokół IKE (Internet Key Exchange) został zaprojektowany w większości przez NSA (National Security Agency) i jest niebywale skomplikowany, głównie ze względu na poziom abstrakcji na jakim operuje (Paterson & Yau, 2006). Wystarczy bowiem włożyć do niego własny zestaw algorytmów kryptograficznych, czy wręcz własną arytmetykę (zestaw ten określa się jako DOI (*Domain of Interpretation*) by otrzymać zupełnie inny od cywilnego protokół, na przykład na potrzeby wojska.

IKE funkcjonalnie składa się z dwóch części: specyfikacji metod kryptograficznych uwierzytelnienia i negocjacji kluczy Oakley oraz specyfikacji formatów pakietów i stanów protokołu ISAKMP. W praktyce nazwy ISAKMP używa się zamiennie z IKE (Paterson & Yau, 2006).

Podstawowe cele IKE to kolejno (za: Paterson & Yau, 2006):

- uwierzytelnienie obu stron komunikacji wobec siebie za pomocą jednej z poniższych metod (ustalanych przez administratora):
    - hasło znane obu stronom (shared secret);
    - podpisy RSA (konieczna ręczna wymiana kluczy publicznych stron);
    - certyfikaty X.509 (najbardziej uniwersalna);
- nawiązanie bezpiecznego kanału dla potrzeb IKE nazywanego ISAKMP SA (Security Association);
- bezpieczne uzgodnienie kluczy kryptograficznych oraz parametrów tuneli IPsec;
- ewentualna ich renegocjacja co określony czas.

Po ustaleniu szczegółów transmisji poprzez IKE obie strony mogą już stworzyć właściwe tunele IPsec i rozpocząć komunikację. Jeśli wymagane jest, by klucze kryptograficzne były regularnie (np. co 8 godzin) zmieniane, IKE również to umożliwia (Paterson & Yau, 2006).

Praktyczną konsekwencją stosowania IKE jest to, że zamiast ręcznego konfigurowania kluczy (a także wielu innych parametrów), administrator może w najprostszym przypadku skonfigurować tylko hasło na obu stronach połączenia, by w pełni automatycznie uzyskać tunele IPsec.

Istotną cechą jest mała ilość informacji, jakie potencjalny atakujący otrzymuje w wyniku podsłuchiwania szyfrowanej komunikacji. Po przechwyceniu zaszyfrowanej transmisji zobaczy bowiem tylko zaszyfrowany pakiet opatrzony dwiema liczbami.

Pierwszą z nich będzie SPI (*Security Parameters Index*), zaś drugą – numer sekwencyjny (Paterson & Yau, 2006). Wartość SPI jest stała, najczęściej generowana losowo i ma kluczowe znaczenie dla stron połączenia. Strony połączenia bowiem na podstawie SPI rozpoznają do jakiej sesji (tunelu) IPsec przynależy dany pakiet i jakie w związku z tym zastosować szyfry oraz klucze do jego rozszyfrowania.

Numer sekwencyjny jest losowany i zwiększany o 1 z każdym wysłanym przez dany kanał pakietem i służy do rozpoznawania pakietów o kolejności przestawionej podczas wędrówki po sieci oraz chroni przed atakami przez powtórzenie (ang. *replay attacks*). Ponieważ numer ten jest wartością 32-bitową, po 2^{32} wysłanych pakietów

kanał musi być zamknięty, a w jego miejsce stworzony nowy, z licznikiem startującym od nowej wylosowanej liczby (Paterson & Yau, 2006).

Inną istotną cechą kanałów IPsec jest ich jednokierunkowość – dany kanał obsługuje tylko ruch idący z hosta A do B. Każda pełna łączność wykorzystuje dwa kanały – jeden od A do B, drugi od B do A. Każdy z nich ma inne SPI, osobny licznik sekwencyjny oraz inne klucze kryptograficzne (Paterson & Yau, 2006).

3.5.4 TUNEL

Mianem tunelu określa się zestawienie połączenia między dwoma odległymi komputerami w taki sposób, by stworzyć wrażenie, że są połączone bezpośrednio (Baczyński, Janoś & Kaczmarek, 2000).

W miarę rozwoju sieci komputerowych pojawiło się zapotrzebowanie na łączenie ze sobą różnych sieci lokalnych za pośrednictwem publicznych sieci rozległych. Pojawiła się jednak kwestia odmiennych standardów, konfiguracji czy też ostatecznie zapewnienia bezpieczeństwa transmisji. Tunelowanie umożliwia bezpieczne przesyłanie pewnych usług sieciowych za pośrednictwem innych, często odmiennych usług sieci, pracujących w różnych standardach (Merike, 2000).

Niezależnie od rodzaju używanych protokołów i celu, jakiemu tunelowanie ma służyć, podstawowa technika pozostaje taka sama. Zwykle jeden protokół służy do ustanowienia połączenia z miejscem zdalnym a drugi do opakowywania danych i instrukcji w celu przesyłania ich przez tunel (Starościak, 2004).

Przykładem wykorzystania tunelu do obejścia niezgodności między protokołami i adresami jest zestaw SIT (*Simple Internet Transition*) który dołączony jest do protokołu IPv6. Technika tunelowania wykorzystana jest na przykład jako narzędzie ułatwiające przechodzenie od wersji 4 protokołu Internetu do jego wersji 6. Wersje IPv4 i IPv6 różnią się od siebie na tyle, że ich bezpośrednie współdziałanie nie jest możliwe. Współdziałanie umożliwia im dopiero zastosowanie tunelowania protokołu IPv4 przez protokół IPv6 i na odwrót (Merike, 2000).

Tunelowanie służy również zabezpieczaniu danych przez utworzenie wokół nich osłony przydatnej podczas przesyłania ich przez domeny pozbawione mechanizmów bezpieczeństwa. Przykładem może być tutaj tunelowanie przez SSH, które polega

na przesyłaniu niezabezpieczonych pakietów protokołów opartych na TCP (np. POP3, SMTP czy HTTP) przez bezpieczny protokół SSH (Laskowski & Wilkołazki, 2005).

Istnieją dwa rodzaje przekierowania portów poprzez tunelowanie po SSH (za: Stallings, 1997):

- lokalne, przekierowujące ruch przychodzący na port lokalny na odpowiedni port zdalny (znajdujący się na innym komputerze w sieci).
  Przykładowo, ruch przychodzący na lokalny port 5000 może zostać przekierowany na port 80;
- zdalne – ruch przychodzący na port na serwerze przekierowywany jest na odpowiedni port lokalny.
  Przykładowo, ruch przychodzący na port 1234 na serwerze może zostać przekierowany na port 23 na komputerze lokalnym.

4

Polityka bezpieczeństwa systemów teleinformatycznych

Cel

Wprowadzenie do polityki bezpieczeństwa informacji. Omówienie podstawowych pojęć oraz terminów wykorzystywanych w dalszej części rozdziału. Klasyfikacja zagrożeń systemów teleinformatycznych. Omówienie i analiza modeli bezpieczeństwa systemów teleinformatycznych.

Plan

1. Podstawowe pojęcia związane z polityką bezpieczeństwa informacji
2. Zagrożenia systemów teleinformatycznych
3. Modele bezpieczeństwa

4.1 PRZEGLĄD PODSTAWOWYCH ZAGROŻEŃ I SPOSOBÓW ZABEZPIECZEŃ SYSTEMÓW TELEINFORMATYCZNYCH

Niektóre przedsiębiorstwa i organizacje żyją dzisiaj w przeświadczeniu, że firewall ochroni je przed wszystkimi zagrożeniami, jakie mogą czyhać na informacje, które firmy posiadają i przetwarzają. Kupowane są systemy wykrywania włamań, ściany ogniowe, oprogramowanie antywirusowe, tworzone są wirtualne sieci prywatne. W większości przypadków poprawia to bezpieczeństwo, ale jedynie w warstwie sieciowej. (Engelmann, 2007)

Zagrożenia bezpieczeństwa systemu teleinformatycznego mogą mieć różnoraki charakter – mogą być dziełem przypadku – wtedy określane są mianem zagrożeń pasywnych, jak i wynikiem celowego działania – tzw. zagrożenia aktywne (Laskowski, 2007). Na każde z nich potrzebny jest inny mechanizm obrony. Wymaga to holistycznego spojrzenia na zagadnienie bezpieczeństwa teleinformatycznego, podczas gdy zazwyczaj gros wysiłków skupiony jest na zapewnieniu bezpieczeństwa stricte pod względem informatycznym, zapominając m.in. o zapewnieniu podstawowego bezpieczeństwa fizycznego czy środowiskowego.

Może się to okazać niewybaczalnym błędem, gdyż osoba atakująca dany system może uzyskać dostęp do poufnych danych przykładowo włamując się do biura lub analizując wydruki, które zostały np. wyrzucone do śmieci (Long, 2008).

W świetle aktualnego prawa większość działań przeciwko zabezpieczeniom systemu informatycznego traktowana jest jako przestępstwo (Fisher, 2000). W szczególności zastosowanie mają tutaj artykuły 266-269 i 287 Kodeksu Karnego. Przykładami takich działań są m.in.:

- włamanie do systemu teleinformatycznego (np. poprzez przejęcie konta administratora bądź użytkownika);
- zniszczenie bądź modyfikacja danych przez osobę niepowołaną;
- nieuprawnione pozyskanie danych (utrata poufności);

- szpiegostwo teleinformatyczne;
- sparaliżowanie pracy systemu np. poprzez atak typu Denial of Service (Szychowiak, 2012);
- podszywanie się pod innego użytkownika;
- utrata autentyczności informacji (np. poprzez przejęcie certyfikatu bądź klucza prywatnego) (Garbarczuk & Świć, 2005).

Zagrożenia bezpieczeństwa systemu informatycznego można podzielić na następujące kategorie (za: Laskowski, 2007):

- fizyczne;
- komunikacyjne (sieciowe);
- związane z oprogramowaniem;
- związane z inżynierią społeczną.

Poniżej omówione zostaną najistotniejsze rodzaje zagrożeń bezpieczeństwa w odniesieniu do poszczególnych elementów systemu teleinformatycznego wraz z najpopularniejszymi sposobami ochrony.

4.1.1 Zagrożenia fizyczne

Zagrożenia fizyczne w systemach teleinformatycznych są najczęściej zagrożeniami pasywnymi, zazwyczaj o charakterze losowym – mogą to być na przykład wyładowania atmosferyczne, pożar, zalanie pomieszczenia, awaria sprzętu komputerowego (Laskowski, 2007).

Należy jednak pamiętać, że równie niebezpieczne są zagrożenia aktywne w postaci fizycznego dostępu osób nieupoważnionych do używanego sprzętu komputerowego i pomieszczeń, w jakich się on znajduje. W przypadku systemów kryptograficznych nawet najsilniejsza metoda szyfrowania może zostać szybko skompromitowana, jeśli podsłuchujący (atakujący) będzie miał fizyczny dostęp do istotnych elementów systemu (np. do klucza szyfrującego bądź tablicy kodowej) lub do używanego w komunikacji sprzętu (Schneier, 2002).

Zagrożenia pasywne mogą być w większości przypadków praktycznie wyeliminowane dzięki właściwie zaplanowanej instalacji: elektrycznej, przeciwpożarowej czy wodno-kanalizacyjnej. W przypadku problemów z zasilaniem najczęściej stosowanymi rozwiązaniami są zasilacze awaryjne (UPS) zdolne podtrzymać pracę systemu przez kilkanaście minut. Istotne systemy teleinformatyczne (a za takie można uznać systemy kryptograficzne) bardzo często wyposażone są w alternatywne źródło (lub źródła) zasilania (Laskowski, 2007).

Wszelkie awarie związane z nieprawidłowym działaniem sprzętu komputerowego są w większości przypadków zjawiskiem losowym i nie sposób przewidzieć ich wystąpienia, jednak ich skutki można zminimalizować poprzez posiadanie np. nadmiarowych (redundantnych) maszyn zapasowych, które relatywnie szybko mogą przejąć rolę uszkodzonych. Z tego samego powodu warto również regularnie wykonywać kopię bezpieczeństwa (backup) danych.

Wszystkie kluczowe urządzenia systemu teleinformatycznego powinny być zabezpieczone w zamkniętych i nadzorowanych pomieszczeniach o ściśle ograniczonym i monitorowanym dostępie. Umożliwi to w dużej mierze wyeliminowanie większości zagrożeń o charakterze aktywnym, choć system ciągle może być narażony na zagrożenia związane z nieostrożnością lub świadomym szkodliwym działaniem uprawnionych użytkowników (Laskowski, 2007). Ten typ zagrożeń zostanie dokładniej omówiony nieco później.

4.1.2 Zagrożenia komunikacyjne (sieciowe)

Przesyłając dane publicznym kanałem komunikacyjnym należy pamiętać, że mogą zostać przechwycone – czy to poprzez fizyczne wpięcie się agresora w sieć, czy też poprzez programy podsłuchujące transmisję (Garbarczuk & Świć, 2005) – ponieważ nikt nie jest w stanie zapewnić bezpieczeństwa na każdym jego odcinku i węźle. Oczywiste jest więc, że wszystkie istotne dane teleinformatyczne powinny być szyfrowane z użyciem silnych metod kryptograficznych.

Co więcej, w przypadku transmisji danych za pomocą sygnałów elektrycznych emitowane jest promieniowanie elektromagnetyczne, które można przechwycić i wykorzystać do bezinwazyjnego podsłuchu. Warto zauważyć, że istnieją również

rozwiązania umożliwiające również podsłuch wizji monitorów (można obejrzeć, nad jakim dokumentem pracuje dany użytkownik), czy transmisji danych do drukarek. W przypadku podsłuchu wizji monitorów nie ma znaczenia typ monitora – choć monitory LCD emitują znacznie mniej promieniowania elektromagnetycznego niż monitory CRT, to jednak sygnał przesyłany przez kabel sygnałowy do karty graficznej jest ciągle możliwy do podsłuchania (pcgate.pl, 2012).

Popularną metodą ochrony systemu teleinformatycznego przed podsłuchem elektromagnetycznym jest oparcie zarówno sieci lokalnej (LAN), jak i połączenia ze światem zewnętrznym o łącze światłowodowe. Innym, dość szeroko rozpowszechnionym rozwiązaniem jest ekranowanie samego komputera (na rynku dostępne są np. specjalnie ekranowane laptopy) . Ekranowane mogą być nawet całe pomieszczenia za pomocą metalowych płyt umieszczonych wewnątrz betonowej konstrukcji ściany. Płyty te dodatkowo są uziemiane – nie jest co po prawda wymagane do zapewnienia skuteczności ekranowania, ale zabezpiecza osoby pracujące w pomieszczeniu przed ryzykiem porażenia prądem wskutek nieszczelności izolacji instalacji elektrycznej. Warto również zauważyć, że pomieszczenie zabezpieczone w ten sposób znacząco zmniejsza ryzyko uszkodzenia znajdującego się w nim sprzętu przed działaniem impulsu elektromagnetycznego – choć ciągle istnieje możliwość przeniknięcia impulsu poprzez instalację elektryczną, teleinformatyczną czy nawet ciepłowniczą (pcgate.pl, 2012).

Jako ciekawostkę można przytoczyć eksperyment polegający na podsłuchu teleinformatycznym (nie zaś elektromagnetycznym) z wykorzystaniem teleskopu (Garbarczuk & Świć, 2005). Na jednym z amerykańskich uniwersytetów postanowiono wycelować teleskop z fotodiodą w zewnętrzny modem stojący przy komputerze w drugim końcu pomieszczenia. Umieszczone na jego obudowie diody sygnalizacyjne transmisji (RX oraz TX) „mrugały" w takt przesyłanych bitów, choć ludzki zmysł wzroku odbierał je jako świecące w sposób ciągły. Okazało się, że tak uzyskany obraz diod sygnalizacyjnych można było bez problemu zamienić na dane na komputerze podsłuchującego.

Do zagrożeń sieciowych można zaliczyć także problematykę kontroli zdalnego dostępu użytkowników do systemu informatycznego oraz jego zasobów (Laskowski, 2007). Rozwiązania tych problemów powinny zostać oparte o grupy uprawnień

(np. za pomocą usług katalogowych) oraz o wiarygodne i trudne do złamania metody uwierzytelnienia użytkownika w systemie (np. klucze SSH, certyfikaty, tokeny, hasła jednorazowe, etc.).

4.1.3 ZAGROŻENIA ZWIĄZANE Z OPROGRAMOWANIEM

W stosunku do każdego rodzaju oprogramowania stosowanego w systemach teleinformatycznych przyjmuje się zasadę ograniczonego zaufania – zakłada się, że oprogramowanie nie jest pozbawione błędów i luk, a jedynie nie zostały one jeszcze wykryte (Saltzer & Schoeder, 1975). Dotyczy to zarówno błędów w systemach operacyjnych, w używanym oprogramowaniu, w zaimplementowanych protokołach czy stosowanych algorytmach. W tym przypadku najprostszym i najbezpieczniejszym rozwiązaniem jest zaktualizowanie używanego oprogramowania do najnowszej wersji najszybciej jak jest to możliwe. W przypadku ryzyka złamania klucza szyfrującego w używanym algorytmie należy znacząco zwiększyć długość używanego klucza do czasu opracowania i zaimplementowania nowego algorytmu kryptograficznego (Schneier, 2002).

Omawiając zagrożenia związane z oprogramowaniem nie należy również zapominać o tzw. złośliwym oprogramowaniu – exploitach, wirusach, trojanach, etc. Zagrożenia tego typu występują najczęściej w dwóch postaciach:

- Pierwszą z nich jest oprogramowanie, które próbuje zaatakować komputer-ofiarę poprzez sieć komputerową. W tym przypadku najprostszym i najpopularniejszym sposobem ochrony jest używanie regularnie aktualizowanego oprogramowania antywirusowego (Garbarczuk & Świć, 2005). Dobrym rozwiązaniem jest również zastosowanie firewalla w celu filtrowania przepływu danych z oraz do sieci – umożliwi to ograniczenie niechcianego ruchu, choć jednak nie oznacza jego całkowitej eliminacji. System chroniony przez zaporę sieciową można przyrównać do zamku otoczonego fosą, przez którą wybudowano kilka mostów (czyli otwartych portów sieciowych). Jeśli intruz będzie chciał się odstać do środka za ich pomocą, atakując uruchomione na nich usługi, firewall go przed tym nie powstrzyma (Zwicky, Cooper & Chapman, 2006).

Należy również zauważyć, że zastosowanie tych dwóch rozwiązań powinno zminimalizować ryzyko wycieku poufnych danych, na przykład za pomocą keyloggera, czyli instalowanego lokalnie programu, który rejestruje wszystkie znaki wpisywane z klawiatury i albo buforuje je na dysku twardym w specjalnym pliku, albo przesyła je przez sieć do komputera osoby podsłuchującej (Laskowski, 2007). W ten sposób dane rejestrowane są przez osobę nieupoważnioną przed ich zaszyfrowaniem, tak więc ani siła ani rodzaj używanego algorytmu szyfrującego nie mają wpływu na bezpieczeństwo tychże danych. Zainstalowanie keyloggera wymaga zazwyczaj fizycznego dostępu do komputera (choć istnieją także trojany wyposażone w funkcję logowania wpisywanych znaków). Warto jednak zanotować, iż w wielu przypadkach program instalacyjny keyloggera wykorzystuje luki w systemach operacyjnych i nie wymaga posiadania uprawnień do instalowania nowego oprogramowania w systemie.

- Drugim rodzajem zagrożenia jest złośliwe oprogramowanie uruchamiane przez użytkownika, w celu uzyskania dostępu do systemu na prawach administratora (eskalacji uprawnień).
- Jednym ze sposobów ochrony jest stosowanie zasady najmniejszego uprzywilejowania: *Każdy program i użytkownik systemu powinien pracować z najmniejszym zestawem przywilejów niezbędnych do wykonania zadania* (Saltzer & Schoeder, 1975).

4.1.4 Zagrożenia związane z inżynierią społeczną

Nawet najlepsze zabezpieczenia i najbardziej wyszkoleni administratorzy systemu mogą okazać się zupełnie bezsilni w starciu z niefrasobliwością użytkowników systemu.

Szczególną rolę odgrywa tutaj socjotechnika. Jest to zestaw metod mających na celu uzyskanie niejawnych informacji przez osobą nieuprawnioną (Mitnick, 2003). Spektrum środków stosowanych przez atakującego może być bardzo szerokie – od podszywania się pod innych użytkowników, poprzez przekupstwo, skończywszy na metodach określanych jako *dumpster diving* – czyli przeszukiwanie śmieci

wyrzucanych przez pracowników atakowanej instytucji w celu znalezienia użytecznych danych (Mitnick, 2003; Long, 2008).

Badania przeprowadzone na potrzeby Infosecurity Europe (BBCEurope, 2004; Leyden, 2003) pokazują, jak groźna może być inżynieria społeczna w połączeniu ze zwykłą ludzką głupotą. Najbardziej skuteczną metodą uzyskania od użytkownika jego hasła dostępu do systemu okazała się być drobna łapówka – dla ponad 70% ankietowanych była to tabliczka czekolady (BBCEurope, 2004), zaś dla 90% – tani długopis (Leyden, 2003).

Co ciekawe, około jedna trzecia respondentów była gotowa podać swoje hasło będąc o to po prostu poproszonym (BBCEurope, 2004).

Często spotykanym problemem jest wykorzystywanie przez użytkowników prostych haseł, łatwych do odgadnięcia bądź złamania. Badania dowodzą, że najczęściej ich rolę pełnią imiona członków rodziny, zwierząt domowych, bądź też nazwa ulubionej drużyny (Long, 2008).

Kolejnym, często wykorzystywanym przez socjotechników przyzwyczajeniem jest ujednolicanie haseł do wielu elementów systemu. Ponad dwie trzecie użytkowników (Leyden, 2003) posiadało identyczne hasło do różnych systemów.

Najczęstszym naruszeniem elementarnych zasad bezpieczeństwa jest jednak zapisywanie haseł otwartym tekstem w ogólnodostępnych miejscach, np. na kartce przyczepionej w miejscu pracy (vide Fot. 4.1).

W tym momencie sztuczki socjotechniczne mogą zostać zastąpione przez spostrzegawczość i pamięć potencjalnego atakującego.

Dodatkowo, kompromitacja hasła może czasami nastąpić w sposób dość spektakularny, jak miało to chociażby miejsce w przypadku Lotniczego Pogotowia Ratunkowego. W głównym wydaniu (o 19:30) Wiadomości TVP w materiale o Lotniczym Pogotowiu Ratunkowym w jednym z kadrów znalazła się biała tablica zlokalizowana w siedzibie LPR (vide Fot. 4.2) – a na niej login i hasło do systemu RescuTrack, którego zadaniem jest monitoring i zarządzanie flotą śmigłowców ratunkowych (Konieczny, 2012). Pomimo, że hasło wygląda na “silne i losowe”, to upublicznienie go (nawet w sposób przypadkowy) w telewizji wartości te przekreśla.

Fot. 4.1. Loginy i hasła dostępowe na kartce przyczepionej do komputera (źródło: opracowanie własne)

Fot. 4.2. Fragment wywiadu telewizyjnego z pracownicą LPR. Zaznaczono login i hasło zapisane na białej tablicy wyraźnie widocznej w kadrze (źródło: Konieczny, 2012)

Podobna sytuacja miała miejsce w 2011 roku w przypadku Prezesa Rady Ministrów Rzeczpospolitej Polskiej. W jednym z programów telewizyjnych znalazło się ujęcie laptopa, z którego korzysta premier wraz z przyklejoną do niego niewielką karteczką z loginem i hasłem (Fot. 4.3). W tym przypadku – na szczęście – nie można mówić o zbyt dużym naruszeniu zasad bezpieczeństwa, gdyż jest to hasło tylko dla użytkownika lokalnego, zaś sam komputer pełni jedynie rolę terminala (niebezpiecznik.pl, 2011).

Fot. 4.3. Login i hasło dostępowe na konto użytkownika lokalnego na kartce przyczepionej do laptopa Prezesa Rady Ministrów (źródło: niebezpiecznik.pl, 2011)

Ciekawa, choć potencjalnie bardziej niebezpieczna sytuacja miała miejsce w przypadku brytyjskiego następcy tronu, księcia Williama, na którego oficjalnej stronie internetowej opublikowano zdjęcia pokazujące go podczas "normalnego dnia pracy" jako pilota helikoptera w Brytyjskich Siłach Lotniczych (Royal Air Force, RAF). Miało to na celu ocieplenie wizerunku przyszłego monarchy. Jednakże bardzo szybko okazało się, że fotografie zawierały coś więcej – na kartkach znajdujących się na drugim planie znajdowały się loginy i hasła do wojskowych systemów (Fot. 4.4a). Oprócz haseł ujawnione zostały także treści e-maila — na jednym ze zdjęć książę William został sfotografowany na tle komputera z otwartym programem pocztowym (niebezpiecznik.pl, 2012).

Pomimo, iż dość szybko zdjęcia księcia skasowano z jego strony, poddano retuszowi i wgrano ponownie w mniejszej rozdzielczości (Fot. 4.4b), kopie

oryginalnych fotografii (wraz z widocznymi loginami i hasłami) zaczęły krążyć w Internecie, co szybko wymusiło na Brytyjskim Ministerstwie Obrony reset haseł do wojskowych systemów.

Pikanterii sprawie dodaje fakt, iż zdjęcia wykonywał wojskowy fotograf, który powinien być świadomy znaczenia tajemnicy wojskowej (niebezpiecznik.pl, 2012).

Fot. 4.4. a) zdjęcia przed retuszem – widoczne loginy i hasła dostępowe (źródło: niebezpiecznik.pl, 2012)

Fot. 4.4. b) zdjęcia po retuszu – zauważalna niższa rozdzielczość (źródło: niebezpiecznik.pl, 2012)

Jednym z najczęściej cytowanych powiedzeń Alberta Einsteina jest: *Tylko dwie rzeczy są nieskończone: wszechświat i ludzka głupota. Co do tej pierwszej są jednak pewne wątpliwości* (Fedirko, 2009).

Jedyną względnie skuteczną metodą obrony przed nieostrożnością użytkowników systemu jest stałe i konsekwentne uświadamianie im zagrożeń płynących z niefrasobliwości. Jednym ze sposobów ochrony jest także opracowanie systemu weryfikacji osób kontaktujących się w sprawach technicznych z użytkownikami systemu, tak, aby zminimalizować ryzyko podszycia się osób trzecich.

4.1.5 Pozostałe zagrożenia bezpieczeństwa

Główne zagrożenia dla systemu informatycznego zostały już wymienione powyżej. Warto rozważyć także wpływ na bezpieczeństwo następujących czynników (za: Szychowiak, 2012; Laskowski, 2007):

- kradzież sprzętu komputerowego (np. laptopa w trakcie podróży służbowej);
- utrata możliwości korzystania z łączy telekomunikacyjnych;
- niedyspozycja administratora lub / i kierownika (np. w skutek jednoczesnej choroby lub urlopu wielu osób);
- niedostępność części zapasowych w serwisie.

4.1.6 Zagrożenia dla systemów teleinformatycznych – podsumowanie

Tabela 4.1. przedstawia listę typowych zagrożeń dla systemów teleinformatycznych.

Rodzaj zagrożenia	Typ zagrożenia	Przyczyna
Zniszczenia fizyczne	Pożar	P, A, Ś
	Zalanie	P, A, Ś
	Zanieczyszczenie	P, A, Ś
	Poważny wypadek	P, A, Ś
	Zniszczenie urządzeń bądź nośników	P, A, Ś
	Pył, korozja, wychłodzenie	P, A, Ś

Rodzaj zagrożenia	Typ zagrożenia	Przyczyna
Zjawiska naturalne	Zjawiska klimatyczne	Ś
	Zjawiska pogodowe	Ś
	Powódź	Ś
Utrata podstawowych usług	Awaria systemu klimatyzacji lub wodno-kanalizacyjnego	P, A
	Utrata zasilania	P, A, Ś
	Awaria urządzeń telekomunikacyjnych bądź teleinformatycznych	P, A
Zakłócenia spowodowane promieniowaniem	Promieniowanie elektromagnetyczne	P, A, Ś
	Promieniowanie cieplne	P, A, Ś
	Impuls elektromagnetyczny	P, A, Ś
Naruszenie bezpieczeństwa informacji	Przechwycenie sygnałów na skutek zjawiska interferencji	A
	Szpiegostwo zdalne	A
	Podsłuch	A
	Kradzież nośników lub dokumentów	A
	Ujawnienie	A
	Odtworzenie z nośników wyrzuconych lub pochodzących z recyklingu	A
	Dane z niewiarygodnych źródeł	A
	Manipulowanie urządzeniem	A
	Sfałszowanie oprogramowania	A
	Detekcja umiejscowienia	A
Awarie techniczne	Awaria urządzenia	P
	Niewłaściwe funkcjonowanie urządzeń	P
	Przeciążenie systemu teleinformatycznego	P, A
	Niewłaściwe funkcjonowanie oprogramowania	P, A
	Naruszenie zdolności utrzymania systemu teleinformatycznego	P, A

Rodzaj zagrożenia	Typ zagrożenia	Przyczyna
Nieautoryzowane działania	Nieautoryzowane użycie urządzeń	A
	Nieuprawnione kopiowanie oprogramowania	A
	Użycie fałszywego lub skopiowanego oprogramowania	A
	Zniekształcenie danych	A
	Nielegalne przetwarzanie danych	A
Naruszenie bezpieczeństwa funkcji	Błąd użytkowania	P, A
	Nadużycie praw	A
	Fałszowanie praw	A
	Odmowa działania	A
	Naruszenie dostępności personelu	P, A, Ś

Tab. 4.1. Lista typowych zagrożeń dla systemu teleinformatycznego
P – zagrożenie pasywne, A – zagrożenie aktywne (rozmyślne), Ś – zagrożenie środowiskowe
(źródło: opracowanie własne na podstawie PN-ISO/IEC 27005:2009)

4.2 STRATEGIA BEZPIECZEŃSTWA

Opracowanie strategii bezpieczeństwa systemu informatycznego stanowi bardzo złożone zadanie. Podobnie jak w przypadku każdego przedsięwzięcia informatycznego, najważniejszym etapem jest etap projektowy.

Wyróżnić możemy jego cztery podstawowe składowe (na podstawie Stallings, 1997; Szychowiak, 2012):

- określenie zasobów systemu (*Co chronić?*);
- oszacowanie ryzyka (*Dlaczego chronić?);*
- identyfikacja zagrożeń (*Przed czym chronić?);*
- analiza kosztów i zysków (*Ile pieniędzy i czasu będzie kosztować ochrona?*).

4.2.1 Określenie zasobów systemu

W zależności od rodzaju instytucji, typu prowadzonej działalności, etc., ochronie powinny podlegać następujące zasoby (za: Stallings, 1997; Szychowiak, 2012):

- sprzęt komputerowy (hardware);
- infrastruktura sieciowa;
- strategiczne dane (w tym dane osobowe i księgowe), zarówno w formie elektronicznej, jak i papierowej;
- wizerunek publiczny i reputacja instytucji;
- kopie zapasowe danych, wersje instalacyjne oprogramowania (ew. także jego kod źródłowy);
- prywatność pracowników;
- zdrowie pracowników.

4.2.2 Oszacowanie ryzyka

Ryzyko ma wiele znaczeń. Potocznie oznacza niepewność, która wiąże się z szansą albo stratą, oznacza jakąś miarę/ocenę zagrożenia czy niebezpieczeństwa wynikającego albo z prawdopodobnych zdarzeń niezależnych, albo z możliwych konsekwencji podjęcia decyzji (Guzik, 2010).

Najogólniej mówiąc, ryzyko jest wskaźnikiem stanu lub zdarzenia, które może prowadzić do strat. Jest ono proporcjonalne do prawdopodobieństwa wystąpienia tego zdarzenia i do wielkości strat, które może spowodować (Guzik, 2010).

W bezpieczeństwie informacji, wg normy ISO/IEC Guide 73:2002, ryzyko jest kombinacją prawdopodobieństwa zdarzenia i jego konsekwencji (następstw), natomiast wg normy ISO/IEC 27005:2008, ryzyko to potencjalna sytuacja, w której określone zagrożenie wykorzysta podatność aktywów lub grupy aktywów powodując w ten sposób szkodę dla organizacji (Guzik, 2010).

Norma ISO/IEC 27001 definiuje wymagania dla systemu zarządzania bezpieczeństwem informacji, który powinien stanowić część składową systemu zarządzania organizacją i być oparty na analizie ryzyka biznesowego. System zarządzania bezpieczeństwem informacji (SZBI) to systematyczne podejście

do zarządzania kluczowymi informacjami w celu zapewnienia ich bezpieczeństwa. Obejmuje on ludzi, procesy, infrastrukturę i systemy informatyczne (sygma.pl, 2012). Ważne jest, aby system uwzględniał cykliczność działań w fazie planowania, wdrażania, weryfikacji i korekty. Norma ta zaleca podejście systemowe zgodnie z cyklem PDCA Deminga (vide Rys. 4.5 i Tab. 4.2) obejmującym następujące aspekty systemu zarządzania bezpieczeństwem informacji (za: Guzik, 2010):

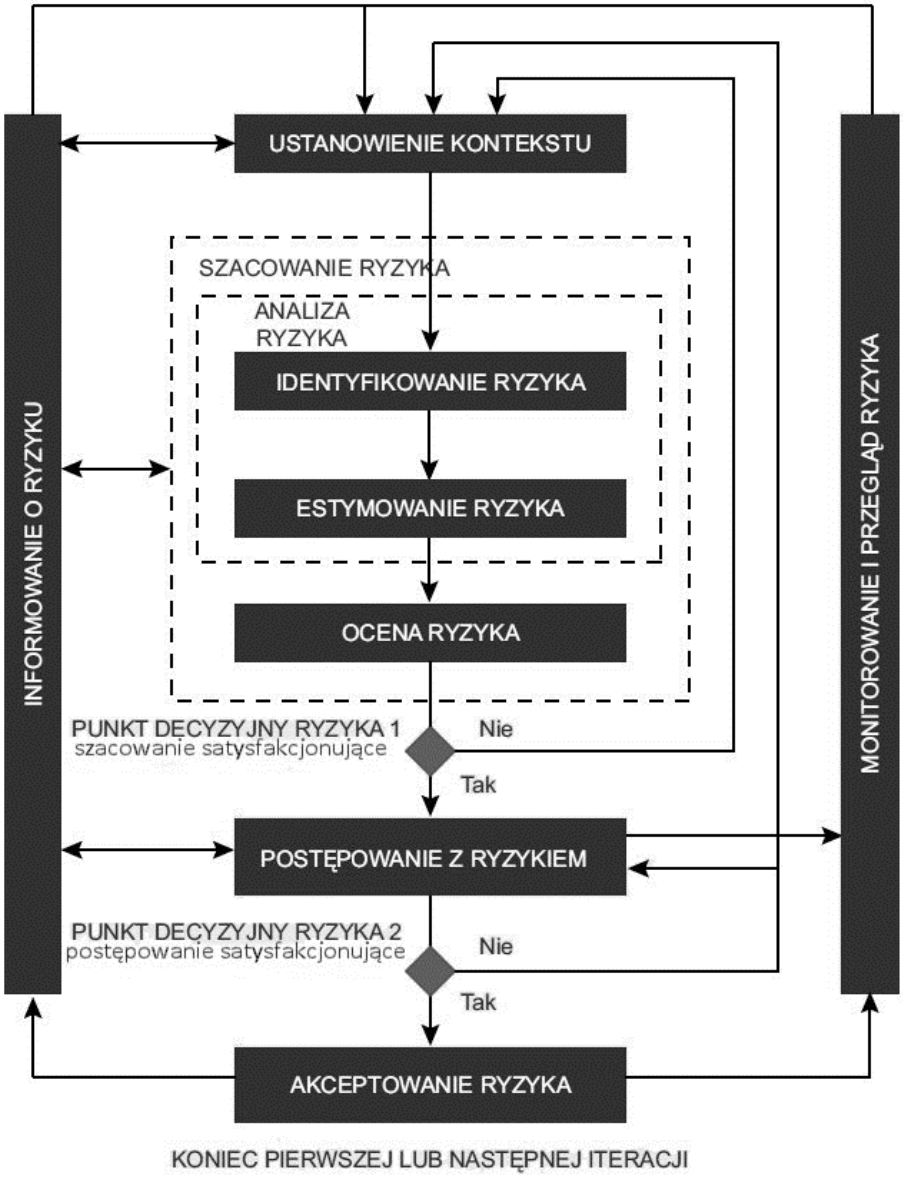
- ustanowienie;
- wdrożenie;
- eksploatację;
- monitorowanie;
- przegląd;
- utrzymanie;
- doskonalenie.

W ramach ustanowienia systemu zarządzania bezpieczeństwem informacji organizacja powinna w kontekście zarządzania ryzykiem wykonać następujące działania (za: Guzik, 2010):

- zdefiniować podejście do szacowania ryzyka w organizacji;
- określić, analizować i oceniać ryzyko;
- zidentyfikować i ocenić warianty postępowania z ryzykiem;
- wybrać cele stosowania zabezpieczeń i zabezpieczenia jako środki postępowania z ryzykiem;
- uzyskać akceptację kierownictwa firmy bądź instytucji dla proponowanych ryzyk szczątkowych.

Sama analiza ryzyka obejmuje (za: Guzik, 2010):

- analizę zasobów;
- analizę zagrożeń;
- analizę podatności;
- analizę zabezpieczeń;
- ocenę (oszacowanie) ryzyk.



Rys. 4.5. Proces zarządzania ryzykiem w bezpieczeństwie informacji (źródło: PN-ISO/IEC 27005:2009)

Proces systemu zarządzania bezpieczeństwem informacji	Proces zarządzania ryzykiem w bezpieczeństwie informacji
Planuj (*Plan*)	Ustanowienie kontekstu
	Szacowanie ryzyka
	Opracowanie planu postępowania z ryzykiem
	Akceptowanie ryzyka
Wykonaj (*Do)*	Wdrożenie planu postępowania z ryzykiem
Sprawdź (*Check)*	Monitorowanie
	Przeglądanie ryzyka
Działaj *(Act)*	Utrzymanie procesu zarządzania ryzykiem w bezpieczeństwie informacji
	Doskonalenie procesu zarządzania ryzykiem w bezpieczeństwie informacji

Tab. 4.2. Relacje pomiędzy procesami systemu zarządzania bezpieczeństwem informacji a procesami zarządzania ryzykiem w bezpieczeństwie informacji (źródło: opracowanie własne na podstawie PN-ISO/IEC 27005:2009)

Istnieją dwie podstawowe metody przeprowadzania analizy ryzyka: kwantyfikatywne oraz kwalifikatywne.

Metody kwantyfikatywne (ilościowe) opierają się na matematycznych obliczeniach wpływu zagrożenia na bezpieczeństwo systemu oraz prawdopodobieństwo jego wystąpienia. Operują wyłącznie na danych numerycznych, opracowanych na podstawie analizy danych statystycznych i historycznych (Piotrowski, 2008).

Metody kwalifikatywne (jakościowe) są znacznie bardziej subiektywne, gdyż bazują na wiedzy i ocenie ekspertów. Wykorzystuje się w nich miary opisowe, które mogą posiadać liczbowe odpowiedniki (Piotrowski, 2008).

Mając zdefiniowaną metodykę analizy ryzyka można przystąpić do zinwentaryzowania zasobów i szacowania ryzyk.

W wyniku przeprowadzonej analizy ryzyka otrzymamy poziomy ryzyk oraz poziom ryzyka akceptowalnego (Guzik, 2010). Zabezpieczenia, jakie należy wdrożyć

w organizacji w celu ograniczenia ryzyk nieakceptowanych, należy opisać w planie postępowania z ryzykiem (Guzik, 2010).

4.2.3 Zagadnienia związane z ryzykiem

Ochrona systemu informatycznego jest podyktowana głównie dwoma aspektami – finansowym oraz obowiązującymi regulacjami prawnymi. Należy bowiem pamiętać, że każde naruszenie bezpieczeństwa systemu może oznaczać potencjalną stratę. Według raportu Computer Security Institute opracowanego we współpracy z FBI, już w roku 2001 186 firm z USA oszacowało szkody powstałe w wyniku włamań do ich systemów teleinformatycznych na prawie 378 milionów dolarów, przy czym najbardziej kosztowna okazała się być kradzież własności intelektualnej (czyli informacji), wyceniona na ponad 151 milionów dolarów (Hatcher, 2001).

Straty mogą mieć również charakter niewymierny – instytucja, która została skompromitowana w wyniku naruszenia bezpieczeństwa systemu traci także wartość bezcenną na rynku – zaufanie klientów (Laskowski, 2007). Część ataków może mieć wyjątkowo złośliwy charakter. Na przykład, agresor może przejąć komputer (lub kilka) w sieci jednej firmy i użyć go (ich) do zaatakowania drugiej.

Dość rozpowszechnione jest także rozsyłanie wiadomości z maszyny-ofiary – dzięki temu atakujący może np. dezinformować kontrahentów atakowanej instytucji (Laskowski & Wilkołazki, 2005).

4.2.4 Regulacje prawne dotyczące bezpieczeństwa teleinformatycznego

Odpowiedź na pytanie *Dlaczego należy chronić?* wydaje się być prosta – taniej jest zainwestować w ochronę, czyli zapobieganie naruszeniom bezpieczeństwa, niż naprawiać powstałe w ich wyniku straty (Laskowski & Wilkołazki, 2005). Dodatkowym bodźcem są tutaj także obowiązujące w Polsce regulacje prawne, które stawiają przed firmami i instytucjami określone wymagania.

W szczególności zastosowanie tutaj mają następujące dokumenty:

- Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych;
- Ustawa z dnia 29 sierpnia 1997 roku o ochronie danych osobowych;

- Ustawa z dnia 29 października 2010 r. o zmianie ustawy o ochronie danych osobowych oraz niektórych innych ustaw;
- Ustawa z dnia 24 sierpnia 2007 r. o zmianie niektórych ustaw w związku z członkostwem Rzeczypospolitej Polskiej w Unii Europejskiej;
- Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne;
- Ustawa z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (wraz z późniejszymi zmianami);
- Ustawa z dnia 27 lipca 2001 roku o ochronie baz danych;
- Ustawa z dnia 16 kwietnia 1993 roku o zwalczaniu nieuczciwej konkurencji (wraz z późniejszymi zmianami);
- Rozporządzenie Prezesa Rady Ministrów z dnia 20 lipca 2011 roku w sprawie podstawowych wymagań bezpieczeństwa systemów i sieci teleinformatycznych;
- Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 roku w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych;
- Rozporządzenie Ministra Sprawiedliwości z dnia 28 kwietnia 2004 roku w sprawie sposobu technicznego przygotowania systemów i sieci służących do przekazywania informacji – do gromadzenia wykazów połączeń telefonicznych i innych przekazów informacji oraz sposobów zabezpieczania danych informatycznych
- Norma PN-ISO/IEC 27001:2007: „Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji – Wymagania", specyfikująca systemy zarządzania bezpieczeństwem informacji. Poza zdefiniowaniem modelu zarządzania bezpieczeństwem informacji, norma PN-ISO/IEC 27001:2007 zawiera opis zabezpieczeń, które należy stosować w celu ograniczenia ryzyka;
- Norma PN-ISO/IEC 17799:2007: „Technika informatyczna – Techniki bezpieczeństwa – Praktyczne zasady zarządzania bezpieczeństwem informacji";
- Norma PN-ISO/IEC 27005:2009: „Technika informatyczna – Techniki bezpieczeństwa – Zarządzanie ryzykiem w bezpieczeństwie informacji".

4.2.5 ANALIZA KOSZTÓW I ZYSKÓW

Projektując strategię bezpieczeństwa należy wziąć pod uwagę fakt, iż w większości przypadków nie przełoży się ona w sposób bezpośredni na zwiększenie zysków firmy czy instytucji.

Głównym celem jej wprowadzenia jest uniknięcie (lub raczej minimalizacja – zawsze istnieje przynajmniej tzw. ryzyko szczątkowe (Laskowski & Wilkołazki, 2005) strat wywołanych naruszeniami bezpieczeństwa.

Można więc przyjąć założenie, że zainwestowane pieniądze będą miały długi – lub nawet bardzo długi – termin zwrotu. Z tego powodu należy dobrze wyważyć wielkość inwestycji w stosunku do chronionego systemu, wartości przechowywanych w nim danych i zakładanego poziomu ryzyka zagrożenia (Schneier, 2002).

Szacując ryzyko należy zidentyfikować i określić granice i wartość istniejącego systemu, a także jego granice i wartość po modyfikacji zabezpieczeń. Warto maksymalnie wykorzystać rozwiązania programowe typu Open Source – w większości są one całkowicie darmowe, bądź też znacznie tańsze od swoich odpowiedników z zamkniętym kodem, co znacząco może wpłynąć na koszt inwestycji, nie obniżając jednocześnie planowanego poziomu bezpieczeństwa (Laskowski & Wilkołazki, 2005).

4.3 POLITYKA BEZPIECZEŃSTWA SYSTEMÓW TELEINFORMATYCZNYCH

Polityka bezpieczeństwa jest zbiorem spójnych, precyzyjnych i zgodnych z obowiązującym prawem przepisów, reguł i procedur, według których dana organizacja buduje, zarządza oraz udostępnia swoje zasoby informacyjne i systemy informatyczne (Bishop, 2004). Jednocześnie określa ona w jaki sposób i które zasoby mają być chronione (Laskowski & Wilkołazki, 2005).

Jako minimum wskazuje się, aby dokument określający politykę bezpieczeństwa zawierał (za: Kaczmarek, 2012):

- definicje bezpieczeństwa informacji, jego ogólne cele i zakres oraz znaczenie bezpieczeństwa jako mechanizmu umożliwiającego współużytkowanie informacji;

- oświadczenie o intencjach kierownictwa, potwierdzające cele i zasady bezpieczeństwa informacji;
- krótkie wyjaśnienie polityki bezpieczeństwa, zasad, standardów i wymagań zgodności mających szczególne znaczenie dla instytucji, np.:
    - zgodność z prawem i wymaganiami wynikającymi z umów;
    - wymagania dotyczące kształcenia w dziedzinie bezpieczeństwa;
    - zapobieganie i wykrywanie wirusów oraz innego złośliwego oprogramowania;
    - zarządzanie ciągłością działania biznesowego;
    - konsekwencje naruszenia polityki bezpieczeństwa;
- definicje ogólnych i szczególnych obowiązków w odniesieniu do zarządzania bezpieczeństwem informacji, w tym zgłaszania przypadków naruszenia bezpieczeństwa;
- odsyłacze do dokumentacji mogącej uzupełniać politykę, np. bardziej szczegółowych polityk bezpieczeństwa i procedur dla poszczególnych systemów informatycznych lub zasad bezpieczeństwa, których użytkownicy powinni przestrzegać.

Polityka bezpieczeństwa ma zazwyczaj rangę oficjalnego, wewnętrznego regulaminu zatwierdzonego przez zarząd instytucji, a przestrzeganie zawartych w nim zasad jest wymagane od wszystkich zatrudnionych w niej osób.

Nad wdrożeniem oraz egzekwowaniem reguł polityki zwykle czuwa wyznaczona do tego osoba, niekiedy określana mianem oficera bezpieczeństwa (np. Schneier, 2002; Bishop, 2004), która jest odpowiedzialna bezpośrednio przed zarządem firmy bądź instytucji i wyposażona w szerokie uprawnienia i pełnomocnictwa.

4.3.1 RÓŻNICE POMIĘDZY POLITYKĄ A STRATEGIĄ BEZPIECZEŃSTWA

Pojęcia polityki i strategii bezpieczeństwa są często błędnie utożsamiane ze sobą. W rzeczywistości oba te terminy uzupełniają się wzajemnie.

Strategia bezpieczeństwa stanowi teoretyczne zaplecze polityki bezpieczeństwa – określa zagrożenia, szacuje ryzyko, definiuje elementy chronionego systemu.

Umożliwia to łatwiejsze sformułowanie zasad i procedur, jakie będą obowiązywać w obrębie danej firmy czy instytucji.

Można powiedzieć, że o ile **strategia bezpieczeństwa** powinna odpowiadać na pytania C*o chronić?*, *Dlaczego chronić?* i *Przed czym chronić*?, o tyle **polityka bezpieczeństwa** musi odpowiedzieć na pytanie *Jak chronić*? (Laskowski, 2007).

4.3.2 WYMAGANIA STAWIANE POLITYCE BEZPIECZEŃSTWA

Głównym celem polityki bezpieczeństwa jest zapoznanie użytkowników systemu z wymaganiami koniecznymi do ochrony zasobów technologicznych i informacyjnych instytucji.

Powinna ona określać mechanizmy, dzięki którym mogą one zostać spełnione, a także uprawnienia poszczególnych grup osób korzystających z systemu. Wszystkie zasady powinny być jasno sformułowane, tak, aby uniknąć dwuznaczności, nieporozumień bądź swobodnych interpretacji reguł przez użytkowników. Z tego powodu jednym ze specyficznych wymagań dotyczących polityki bezpieczeństwa jest język, jakim jest ona napisana – musi być on zrozumiały dla wszystkich, których ona dotyczy (Bishop, 2004).

Co więcej, powinna również wyjaśniać powody stosowania określonych środków i metod ochrony (Zwicky, Cooper & Chapman, 2006). Polityka bezpieczeństwa jako dokument będzie skuteczna tylko wtedy, kiedy może zostać w pełni zrozumiała przez odbiorców – poza odpowiedzią na pytanie *Jak chronić*? musi też mówić *Dlaczego?* (Bishop, 2004).

Polityka bezpieczeństwa powinna określać zakres obowiązków wszystkich grup użytkowników – każda osoba mająca dostęp do systemu odpowiada za jego bezpieczeństwo, ale w różnym zakresie (Laskowski & Wilkołazki, 2005).

Staranne i jednoznaczne rozdzielenie funkcji i odpowiedzialności jest więc sprawą kluczową. Co więcej, należy również sprecyzować kto i jakie działania może podjąć w przypadku nie przestrzegania obowiązujących zasad. Wiele instytucji, zwłaszcza komercyjnych, definiuje również dopuszczalny zakres wykorzystywania firmowych komputerów do celów prywatnych (Bishop, 2004).

System informatyczny ulega ciągłym modyfikacjom. Wdrażane są nowe rozwiązania, oprogramowanie, technologie. Niemożliwe jest określenie wszystkich kierunków zmian, jak również nie można przewidzieć wszystkich sytuacji, które mogą wystąpić podczas eksploatacji systemu. Twórcy polityki bezpieczeństwa powinni więc uwzględnić jej okresowe rewizje (aktualizacje), jak również określić proces uwzględniania wyjątków oraz wyznaczyć osoby mające w takiej sytuacji prawo do działania (Bishop, 2004).

Integralną częścią dokumentu powinny być także procedury działania, tak w sytuacjach kryzysowych, jak i w przypadku codziennej eksploatacji systemu. Scenariusze powinny charakteryzować się swoistą nadmiarowością, przewidując działania także w szczególnie złożonych przypadkach, np. co robić, jeśli schemat przewiduje wezwanie administratora, a ten pozostaje nieosiągalny (Fisher, 2000).

W literaturze (Laskowski, 2007) sugeruje się także, aby regulamin zawierał zakres informacji utajnionych, np. związanych z topologią sieci, zastosowanymi technologiami, etc. Dobrym rozwiązaniem wydaje się być zawarcie tych danych w osobnej dokumentacji systemu, wgląd do której będą posiadać jedynie osoby upoważnione.

Najważniejszym wymogiem stawianym przed polityką bezpieczeństwa jest jednak jej akceptacja przez wszystkich użytkowników systemu – każdy z nich powinien otrzymać ten dokument w formie pisemnej, potwierdzając zapoznanie się z nim własnoręcznym podpisem.

4.3.3 Elementy polityki bezpieczeństwa

Amerykański Narodowy Instytut Standardów i Technologii wyróżnił następujące elementy, jakie powinna zawierać poprawnie skonstruowana polityka bezpieczeństwa systemu teleinformatycznego (za: NIST, 1995):

- identyfikacja i uwierzytelnianie;
- kontrola dostępu;
- śledzenie odpowiedzialności;
- audyt stanu bezpieczeństwa;
- ochrona współdzielonych zasobów;

- dokładność i niezawodność;
- ochrona komunikacji.

Identyfikacja i uwierzytelnianie

Identyfikacja i uwierzytelnianie określają mechanizmy autoryzacji użytkowników w systemie. Są one zaimplementowane we wszystkich współczesnych sieciowych systemach operacyjnych. Dla wzmocnienia niezawodności i siły uwierzytelniania osób podających się za prawowitych użytkowników skonstruowano wiele ciekawych rozwiązań technicznych opierających się na personalnych generatorach tymczasowych haseł bądź nawet bezpośrednim pomiarze danych biometrycznych (iniejawna.pl, 2012).

Kontrola dostępu

Kontrola dostępu sprowadza się zazwyczaj do określenia praw poszczególnych osób do korzystania z zasobów systemu. Mogą one zabraniać dostępu do określonych elementów (plików, programów, urządzeń, etc.) bądź ograniczać go tylko do podzbioru dozwolonych operacji, jakie użytkownik może na nich wykonać (Laskowski & Wilkołazki, 2005).

Mechanizmy zapewniające taką kontrolę mogą mieć różnoraką naturę. W grę wchodzą tu zarówno rozwiązania ograniczające fizyczny dostęp do nośników i urządzeń, jak również zabezpieczenia systemowe zaimplementowane w oprogramowaniu (iniejawna.pl, 2012).

Śledzenie odpowiedzialności

Polega na możliwości odtworzenia historii operacji wykonanych w systemie w powiązaniu z jednoznaczną identyfikacją użytkowników, którzy je zainicjowali oraz czasem wykonania. Również te operacje, które zostały wykonane w sposób niedozwolony, omijając zabezpieczenia systemu (co uniemożliwia bezpośrednią identyfikację sprawcy) muszą być śledzone w celu zbadania stopnia ich szkodliwości oraz przywrócenia pierwotnego stanu systemu (iniejawna.pl, 2012).

Audyt stanu bezpieczeństwa

To istotne zadanie powinno być wykonywane regularnie w celu utrzymywania zabezpieczeń systemu w stanie wysokiej gotowości. Ze względu na dynamicznie zmieniające się środowisko działania systemów, wciąż wykrywane luki w zabezpieczeniach oraz niesłabnącą pomysłowość włamywaczy skuteczność wykorzystywanych zabezpieczeń powinna być ciągle monitorowana i poprawiana.

Jest to jeden z powodów ciągle rosnącej popularność systemów wykrywania włamań i testowania zabezpieczeń, które na zasadzie sprzężenia zwrotnego potrafią modyfikować ich konfigurację w celu uzyskania pewniejszej ochrony (iniejawna.pl, 2012).

Ochrona współdzielonych zasobów

Stanowi rozwinięcie zagadnienia kontroli dostępu, dotyczy zaś tej grupy zasobów, która z racji ich współdzielenia przez wielu użytkowników jest szczególnie wrażliwa na zachowania naruszające zasady dobrej współpracy (Laskowski, 2007).

Dokładność i niezawodność ochrony

Elementy te mają zapewnić systemowi odporność na wszelkie próby zmonopolizowania jego zasobów przez uprzywilejowanego użytkownika działającego w sposób nieudolny bądź nierozważny, jak również oddalić groźbę przejęcia kontroli nad systemem przez osoby nieuprawnione w sytuacji kryzysowej.

Sytuacja taka może przykładowo mieć miejsce w warunkach nietypowych, takich jak poważna awaria systemu zasilania bądź wystąpienie krytycznego błędu aplikacji użytkowej (iniejawna.pl, 2012).

Ochrona komunikacji

Ochrona komunikacji jest tematem, który często mylnie utożsamiany jest z całokształtem ochrony systemów teleinformatycznych (Laskowski, 2007).

W rzeczywistości element ten skupia się na zachowaniu integralności i poufności danych transmitowanych wewnątrz sieci lokalnej (pomiędzy elementami systemu), jak również do zapewnienia możliwości bezpiecznej komunikacji z systemem użytkownikowi znajdującemu się poza nim.

Taką możliwość zapewnia m.in. tzw. wirtualna sieć prywatna (ang. *Virtual Private Network*, VPN), którą można opisać jako "tunel", przez który płynie ruch w ramach sieci prywatnej pomiędzy klientami końcowymi za pośrednictwem publicznej sieci (takiej jak Internet) w taki sposób, że węzły tej sieci są przezroczyste dla przesyłanych w ten sposób pakietów.

Taki kanał może opcjonalnie kompresować i/lub szyfrować dane w celu zapewnienia lepszej jakości przesyłu lub zwiększenia poziomu bezpieczeństwa (Laskowski & Wilkołazki, 2005).

'Wirtualna oznacza, że sieć ta istnieje jedynie jako struktura logiczna działająca w ramach rzeczywistej sieci publicznej, w odróżnieniu do sieci prywatnej, która powstaje na bazie specjalnie dzierżawionych w tym celu łącz.

Pomimo takiego mechanizmu działania stacje końcowe mogą korzystać z VPN dokładnie tak, jak w sytuacji gdyby istniało pomiędzy nimi fizyczne łącze prywatne (Laskowski & Wilkołazki, 2005).

Rozwiązania oparte na VPN powinny być stosowane w firmach, których pracownicy pracują zdalnie ze swoich domów lub łączą się z siecią firmy podczas wyjazdów służbowych, przez nie zabezpieczone łącza.

Co więcej, warto zastosować sieć VPN w przypadku, gdy firma wykorzystuje sieć bezprzewodową, gdyż sieci tego typu przez swoją specyfikę są bardzo narażone na podsłuch i dostęp osób nieupoważnionych. Zastosowanie VPN w tej sytuacji pozwala na wiarygodne uwierzytelnianie użytkowników oraz silne szyfrowanie przesyłanych danych (Laskowski & Wilkołazki, 2005).

Wirtualne sieci prywatne charakteryzują się dość duża efektywnością, nawet na słabych łączach (dzięki kompresji danych) oraz wysokim poziomem bezpieczeństwa (ze względu na szyfrowanie) (Laskowski & Wilkołazki, 2005).

4.3.4 IMPLEMENTACJA POLITYKI BEZPIECZEŃSTWA

Wdrożenie w życie polityki bezpieczeństwa również musi zostać przeprowadzone według określonego zbioru procedur.

Tworząc ten zestaw należy wziąć pod uwagę następujące czynniki:

- **fizyczny nadzór nad bezpieczeństwem teleinformatycznym**;

  Odnosi się on do fizycznych aspektów chronionego systemu: infrastruktury, zabezpieczeń oraz dostępu (Merike, 2000).

  W przypadku sieci komputerowej fizyczna infrastruktura odnosi się zarówno do stosowanego rodzaju nośnika, jak i do topografii sieci (Laskowski, 2007). Istotnym elementem jest również bezpieczeństwo urządzeń, na które składa się zidentyfikowanie ich lokalizacji, ograniczenie dostępu osób nieupoważnionych, ale także rozmieszczenie zabezpieczeń środowiskowych (np. systemów przeciwpożarowych, kontroli temperatury i wilgotności, dodatkowych źródeł zasilania, etc.). Aspektem fizycznego nadzoru, który często jest pomijany bądź marginalizowany jest ochrona okablowania strukturalnego, zarówno przed uszkodzeniem, jak i przed nieautoryzowaną modyfikacją (Laskowski, 2007).

- **logiczny nadzór nad bezpieczeństwem teleinformatycznym**;

  Tworzy granice pomiędzy segmentami sieci (na przykład poprzez podział na podsieci). Należy pamiętać jednak, iż logiczne (programowe) rozdzielenie elementów nie jest tak silne, jak podział fizyczny, powinno być więc dobrze zaplanowane.

  Dostęp logiczny (poprzez oprogramowanie) powinien podlegać kontroli tak samo, jak dostęp fizyczny.

  Według (Merike, 2000) należy zaimplementować dwa rodzaje nadzoru logicznego:

  - prewencyjny – zaprojektowany do jednoznacznego identyfikowania autoryzowanych użytkowników, ale także do odmowy dostępu dla osób nieautoryzowanych;
  - wywiadowczy – pełniący rolę raportową.

- **integralność systemu teleinformatycznego i znajdujących się w nim danych**;
  Te dwa czynniki są szczególnie ważne przy wdrażaniu polityki bezpieczeństwa do istniejącego i działającego systemu komputerowego. Osoby odpowiedzialne za implementację powinny kierować się znaną lekarską zasadą *primum non nocere* – czyli *po pierwsze nie szkodzić*.
  Priorytetowym działaniem powinno być zachowanie ciągłości pracy systemu. Co więcej, wszelkie zmiany powinny być maksymalnie transparentne z punktu widzenia użytkownika. Z tego powodu sugerowane jest, aby modyfikacje wymagające przerw w działaniu systemu były wdrażane poza standardowymi godzinami pracy (Bishop, 2004).
  Drugim priorytetem powinno być zachowanie integralności danych. W trakcie wdrażania zmian do systemu znajdujące się w nim dane użytkownika nie mogą zostać zmodyfikowane.
  Można jednak wyznaczyć pewne odstępstwa od tej zasady. Dotyczy to na przykład sytuacji, kiedy dane zostaną zaszyfrowane. Innym dosyć często występującym przypadkiem jest ich przeniesienie – konta użytkowników z wielu maszyn są grupowane na jednej. W tej sytuacji należy zwrócić szczególną uwagę na zachowanie poufności danych podczas transferu. Dodatkowo, warto zabezpieczyć je przed przypadkowym uszkodzeniem tworząc kopię zapasową (Laskowski, 2007).

4.4 MODEL BEZPIECZEŃSTWA

Z problematyką bezpieczeństwa systemu informatycznego powiązane jest także pojęcie modelu bezpieczeństwa. Wyraża ono w sposób sformalizowany, precyzyjny i jednoznaczny te aspekty polityki bezpieczeństwa, których realizacja jest wymagana w systemie informatycznym.

Wyróżnia się pięć podstawowych modeli (za: Schneier, 2002; Bishop, 2004; Laskowski, 2007):

- model zerowy – oznaczający brak jakichkolwiek zabezpieczeń, stosowany jest głównie w organizacjach, w których założono, że poziom ryzyka zagrożenia jest

niewspółmiernie niski w stosunku do kosztów opracowania i wdrożenia polityki bezpieczeństwa;

- zabezpieczenie przez utajnienie (ang. *security by obscurity*) opiera się o założenie, że jeśli nikt nie będzie wiedział (lub bardzo mało będzie wiadomo) o istnieniu systemu komputerowego (i o jego wadach), to ryzyko naruszenia bezpieczeństwa będzie minimalne;
- zabezpieczenie przez niepozorność (ang. *security by inconspicuity*) opiera się o socjotechniczne założenie, że jeśli system informatyczny będzie wyglądał na mało istotny (pełniący mało znaczącą rolę), to nikt nie będzie zainteresowany przełamywaniem jego zabezpieczeń;
- zabezpieczenie systemu na poziomie poszczególnych komputerów (ang. *my home is my castle)* – ten model zakłada, iż każdy użytkownik w systemie odpowiada za bezpieczeństwo swojej maszyny i przechowywanych w niej danych;
- zabezpieczenie systemu na poziomie całej sieci (ang. *whole network security*), polegające na kontrolowaniu dostępu do i z sieci poszczególnych komputerów i oferowanych przez nie usług. Model ten obejmuje także tworzenie firewalla (bądź wielu firewalli) oraz używania skutecznych metod uwierzytelniania i szyfrowania transmisji w sieci.

4.4.1 Wady i zalety omówionych modeli bezpieczeństwa

Poddając analizie przedstawione powyżej modele bezpieczeństwa można zauważyć, że trzy pierwsze charakteryzują się całkowicie błędnymi założeniami. Instytucja, która nie podejmuje żadnych działań w celu zabezpieczenia swojego systemu, cechuje się wyjątkową krótkowzrocznością – koszty usunięcia skutków ewentualnego ataku będą zdecydowanie większe niż środki, które należałoby wydać na wprowadzenie odpowiedniego poziomu bezpieczeństwa.

Zabezpieczanie poprzez utajnianie może być stosowane jako jeden z elementów składowych polityki, nie zaś jako jej zastępstwo. Nie jest możliwym ukrycie w sposób całkowity obecności danego komputera w sieci, nawet łącząc wiele różnych metod maskujących. Należy tutaj również wspomnieć, iż ten sposób zabezpieczenia łamie jedną z podstawowych zasad zaczerpniętych ze współczesnej kryptografii – **regułę**

Kerckhoffsa, mówiącą, że system powinien być bezpieczny nawet wtedy, kiedy wszystkie jego elementy (za wyjątkiem klucza dostępu) są powszechnie znane (Kerckhoffs, 1883).

Założenie, że jeśli coś nie wygląda na warte kradzieży, to nie zostanie ukradzione, w przypadku systemów komputerowych jest błędne. Wynika to głównie z faktu, że w wielu przypadkach zaatakowany system nie jest celem sam w sobie, lecz jest używany jako środek w ataku na inny komputer, np. jako element tzw. botnetu, czyli grupy komputerów zainfekowanych złośliwym oprogramowaniem (np. robakiem) pozostającym w ukryciu przed użytkownikiem i pozwalającym agresorowi na sprawowanie zdalnej kontroli nad wszystkimi zarażonymi przez niego komputerami (Laskowski, 2007).

Główną wadą modelu opartego na zabezpieczeniu systemu na poziomie poszczególnych komputerów jest przeniesienie głównego ciężaru odpowiedzialności za bezpieczeństwo na zwykłych użytkowników. Może to skutkować bardzo nierównym poziomem ochrony konkretnych maszyn znajdujących się w sieci.

Drugą bardzo poważną wadą jest słaba skalowalność tego rozwiązania, która ujawnia się zwłaszcza przy różnorodnej strukturze sprzętowo-programowej (Laskowski & Wilkołazki, 2005).

Model zakładający zabezpieczenie systemu na poziomie całej sieci jest znacznie bardziej efektywny niż pozostałe. Jest dosyć łatwo skalowalny – pozwala rozbudowywać system o dowolną liczbę hostów (o ile jest to możliwe ze względu na infrastrukturę instytucji) bez obniżenia poziomu bezpieczeństwa. Jego efektywność może zostać dodatkowo zwiększona poprzez dostosowanie zabezpieczeń na poziomie poszczególnych komputerów do obowiązujących na poziomie całej sieci. Dzięki temu każdy z użytkowników może dodatkowo zabezpieczyć swoją maszynę pozytywnie wpływając na ogólny poziom bezpieczeństwa.

5

Kierunki rozwoju technik ochrony informacji

Cel

Omówienie podstawowych pojęć oraz technik kryptografii kwantowej. Omówienie i analiza ogólnych problemów związanych z dwuskładnikowym uwierzytelnieniem.

Plan

1. Kryptografia kwantowa
2. Kryptologia kwantowa
3. Uwierzytelnianie dwuskładnikowe

5.1 KRYPTOGRAFIA KWANTOWA

Kryptografia kwantowa obejmuje metody wykonywania zadań kryptograficznych przy użyciu hipotetycznej informatyki kwantowej, która zajmuje się wykorzystaniem możliwości układów kwantowych do przesyłania i obróbki informacji kwantowej (Grabowski, 2003).

Podstawową jednostką obliczeniową wykorzystywaną w informatyce kwantowej jest kubit (bit kwantowy). Obliczenia kwantowe opisywane są za pomocą bramek kwantowych, których działanie jest odwracalne (Grabowski, 2003).

5.1.1 SZYFROWANIE KWANTOWE

Szyfrowanie kwantowe służy do przekazywania danych na niewielkie odległości (do kilkudziesięciu kilometrów) za pomocą światła.

Zgodnie z prawem niepewności Heisenberga, nie istnieje możliwość dokładnego zmierzenia dwóch wzajemnie zależnych wielkości opisujących stan cząstki elementarnej, bez zmiany choćby jednej z nich. Zasada ta leży u podstaw kryptografii kwantowej. Przykładem wielkości, których nie da się jednoznacznie określić w jednym momencie czasu jest np. prędkość i położenie fotonu. Z punktu widzenia kryptografii wygodniejsze jest posłużenie się kątami polaryzacji (kierunkami drgania) fotonów. To na nich właśnie opiera się opracowany w 1984 r. protokół BB84 wykorzystujący prawo niepewności kwantowej do bezpiecznej wymiany kluczy szyfrujących pomiędzy odległymi od siebie stronami (Grabowski, 2003).

Foton może być spolaryzowany prostokątnie – pionowo lub poziomo – lub też ukośnie – pod kątem 45 lub 135 stopni. Płaszczyzny polaryzacji, zwane też bazami, oznaczane są następująco (za: Grabowski, 2003):

+ – baza prostokątna

x – baza ukośna

Kierunki polaryzacji fotonów oznaczane są zaś w następujący sposób (za: Grabowski, 2003):

| – kierunek pionowy
– – kierunek poziomy
\ – kierunek ukośny lewy
/ – kierunek ukośny prawy

Jeżeli foton jest spolaryzowany prostokątnie, kąt jego polaryzacji można poprawnie zmierzyć jedynie przy pomocy odbiornika mierzącego polaryzację prostokątną. Jeżeli zaś foton jest spolaryzowany ukośnie, kąt jego polaryzacji można poprawnie zmierzyć jedynie przy pomocy odbiornika ustawionego na odbiór ukośny. Jeżeli więc foton drga w jednym z kierunków prostokątnych, pomiar polaryzacji przy bazie ukośnej będzie błędny – i odwrotnie (Grabowski, 2003)

Zakładając, że Ewa chce podsłuchać wiadomość składającą się tylko z 1 bitu, ustawia więc swój polaryzator w dowolnej pozycji wyjściowej. Foton ma 50% szans na przekazanie wiadomości (statystycznie 50% fotonów przejdzie przez źle ustawiony polaryzator) (Garbarczuk & Świć, 2005).

Jeżeli Ewa „trafi" w ustawienie, foton przekaże właściwą informację. Jednak ponieważ Ewa nie jest w stanie określić, w których przypadkach polaryzator jest ustawiony dobrze, a w których źle, nie jest również w stanie odszyfrować wiadomości.

5.1.2 Wymiana kluczy w kryptografii kwantowej

Głównym pomysłem w kwantowej wymianie kluczy jest użycie najmniejszych możliwych porcji energii do przekazania informacji (kubitów).

Każda próba odczytu informacji powoduje jej bezpowrotne zniszczenie. Nie istnieje sposób przechwycenia transmisji bez jej zakłócenia, więc kluczowe informacje mogą być wymieniane z dużą pewnością zachowania tajemnicy.

Algorytm wymiany kluczy można opisać w następujący sposób (za: Grabowski, 2003):

1. Alice losuje klucz i przesyła go Bobowi poprzez losowo ustawione nadajniki;
2. Bob za pomocą losowo ustawionych detektorów odbiera transmisję od Alice;
3. Bob jawnym kanałem przekazuje, w jaki sposób ustawił swoje detektory;
4. Bob mógł jednak źle odczytać polaryzację albo też część fotonów w ogóle do niego nie dotarła (puste pola w tabeli 5.1.). W każdym razie, wartości, które zostały odczytane prawidłowo mogą, po powtórzeniu podobnych prób potrzebną ilość razy, utworzyć po każdej ze stron klucz szyfrujący dla sesji. Alice informuje Boba, w których przypadkach się pomylił.
5. Bob i Alice jawnym kanałem porównują co najmniej kilkadziesiąt bitów z uzyskanego klucza – jeżeli dojdą do wniosku, że komunikacja szyfrowana ustanowionym w ten sposób kluczem przestała być bezpieczna (rosnąca liczba fotonów, których polaryzacja została nieprawidłowo odczytana pomimo zgodności ustawień nadajnika i odbiornika, co może sugerować podsłuch), procedura generowania klucza jest powtarzana. Dla podwyższenia bezpieczeństwa transmisji, rzeczywisty klucz może zostać utworzony przez zastosowanie dowolnej funkcji skrótu.

Alice wysyła do Boba:	-	|	>	>	|	-	<	-	|	|	>	<
Bob ustawia odbiornik:	+	X	+	X	X	X	+	X	X	+	+	+
Bob odczytuje:	-	<	-	>	>	>		<	<			
Bob przekazuje Alice:	+	X	+	X	X	X		X	X			
Alice odpowiada:	OK			OK								

Tab.5.1. Przykładowe wartości polaryzacji przekazywane przez Alice do Boba (źródło: Grabowski, 2003)

5.1.3 KRYPTOANALIZA KWANTOWA

Omawiając temat kryptografii kwantowej warto również wspomnieć o zagrożeniach, jakie niesie ze sobą kryptoanaliza kwantowa.

Za pomocą hipotetycznych komputerów kwantowych możliwe byłoby relatywnie szybkie (w porównaniu do „zwykłych" komputerów) dokonywanie pewnych obliczeń, np. faktoryzacji dużych liczb algorytmem Shora, co pozwoliłoby np. na złamanie RSA (Garbarczuk & Świć, 2005).

Kryptografia kwantowa pozostaje aktualnie głównie domeną badań akademickich – choć na rynku pojawiły się pierwsze systemy kryptograficzne, oferujące oparte o nią rozwiązania (Garbarczuk & Świć, 2005). Jednak ich cena oraz stosunkowo małe możliwości zastosowania (ograniczenie możliwości przesyłu informacji do ok. 200 kilometrów (Garbarczuk & Świć, 2005) jeszcze przez długi czas będą stanowić barierę przed ich powszechnym zastosowaniem.

5.2 WIELOPLATFORMOWE TECHNIKI OCHRONY INFORMACJI

Dwustopniowe uwierzytelnianie jest jedną z najpopularniejszych obecnie technik ochrony informacji, szczególnie w odniesieniu do uwierzytelnienie tożsamości użytkownika. Idea tej techniki jest prosta: użytkownik np. weryfikuje swoją tożsamość używając nie tylko hasła, ale także drugiego elementu uwierzytelniającego.

Istnieje wiele różnych czynników, które mogą zostać wykorzystane jako element uwierzytelniający użytkownika (za: Pieprzyk, Hardjono & Seberry, 2006):

- *Coś, co użytkownik zna* – np. hasło, PIN czy wzorzec (np. wzór, jaki trzeba narysować, aby odblokować smartfon);
- *Coś, co użytkownik posiada* – może to być np. token, karta chipowa lub magnetyczna, kod sms, hasło z tablicy haseł jednorazowych, etc.
- *Coś, czym użytkownik jest* – czyli wszelkiego rodzaju czynniki biometryczne – odcisk palca, skan siatkówki, etc.

Dwustopniowe uwierzytelnianie jest stosowane obecnie przez wiele firm i serwisów internetowych (m.in. Google Mail czy Dropbox).

Jednym z ciekawszych (ze względu na skalę zastosowania) przypadków użycia dwuskładnikowego uwierzytelniania jest 3-D Secure, czyli metoda autoryzacji transakcji dokonywanych bez fizycznego użycia karty stosowana przez Visa i MasterCard, mająca na celu zwiększenie bezpieczeństwa oraz zaufania do płatności kartami w Internecie.

3-D Secure jest standardem zabezpieczenia transakcji poprzez identyfikację właściciela karty przy użyciu dodatkowego, najczęściej jednorazowego hasła wygenerowanego przez token lub otrzymanego via SMS. Tego hasła nie używa się przy transakcjach wymagających fizycznej obecności karty, stąd nigdy nie jest ono identyczne z PIN (Engelmann, 2007).

Wstępna autoryzacja transakcji jest dokonywana bezpośrednio poprzez bank – wystawcę karty np. poprzez dodatkowe hasło. Bank po potwierdzeniu, że osoba dokonująca zakupu jest rzeczywistym posiadaczem karty kieruje transakcję do normalnej autoryzacji. Całkowitą odpowiedzialność za transakcję dokonaną przy użyciu 3D Secure ponosi właściciel karty (Engelmann, 2007).

Warto zauważyć, że dwuskładnikowe uwierzytelnienie nie jest jednak całkowicie bezpieczne. System ten podatny jest na atak chociażby w wyniku zarażenia komputera użytkownika złośliwym oprogramowaniem (kopalniawiedzy.pl, 2009) bądź też kradzieży urządzenia uwierzytelniającego lub przechwycenia transmisji.

POSŁOWIE

Upowszechnienie PGP nie oznaczało końca wojny o powszechność kryptografii. Przeciwnie – wydarzenia 11 września 2001 sprawiły, że rozgorzała ona z nowa i jeszcze większą siłą.

Zarówno w Kongresie USA jak i w Parlamencie Europejskim pojawiły się głośne inicjatywy, które zmierzają do wprowadzenia ograniczeń dostępności oprogramowania umożliwiającego skuteczne szyfrowanie i ograniczające możliwości ochrony informacji, zwłaszcza w sferze prywatności zwykłych użytkowników Internetu. Tłumaczy się to dobrem publicznym oraz możliwością wykrycia organizacji i działań terrorystycznych.

Pojawiają się również idee żądające ogólnoświatowej prohibicji na programy pozbawione tzw. backdoorów, czyli rozwiązań, które umożliwiłyby organizacjom rządowym i różnego rodzaju służbom inwigilacje treści przekazywanych droga elektroniczną.

Istnieje także kontrowersyjny system szpiegowania ogólnoświatowej sieci, jaką jest Internet.

Nie powinniśmy pozostać na to obojętni.

Jak mówią Amerykanie – *Stay tuned*.

Jeszcze wiele przed nami.

Lublin, listopad – grudzień 2012

BIBLIOGRAFIA

Abramson, N. (1963). *Information theory and coding.* McGraw-Hill.

Baczyński, T., Janoś, T. & Kaczmarek, S. (2000). *Vademecum Teleinformatyka.* IDG Poland.

BBCEurope. (2004). *Passwords revealed by sweet deal*. Pobrano 15.11.2012 z lokalizacji http://news.bbc.co.uk/2/hi/technology/3639679.stm

Bishop, M. (2004). *Computer security: art and science.* Addison-Wesley.

Blackman, C. (2009, 07 17). Chance of nuclear war is greater than you think: Stanford engineer makes risk analysis. *Stanford Report* .

Byrski, M. (1985). *Kamasutra, czyli traktat o miłowaniu w przekładzie Marii Krzysztofa Byrskiego.*

Cackowski, Z., Kmita, J. & Szaniawski, K. (red.). (1987). *Filozofia a nauka.* Wrocław – Warszawa – Kraków – Gdańsk – Łódź: Ossolineum.

Childs, J. (2000). *General Solution of the ADFGVX Cipher System.* Aegean Park Press.

Courtois, N. (2011). *Security Evaluation of GOST 28147-89 In View Of International Standardisation.* Pobrano z lokalizacji http://eprint.iacr.org/2011/211

Cryptologia. (2005). *Cryptologia vol. XXIX* , s.47.

Diffie, W. & Hellman, M. (1976, 11). New Directions in Cryptography. *IEEE Transactions on Information Theory* , strony 644-654.

Donaldson, G. (1974). *Mary, Queen of Scots.* Londyn: English Universities Press.

Doyle, A. (2011). *Powrót Sherlocka Holmesa.* Wydawnictwo Algo.

ed-thelen.org. (2012). *Enigma Rotors.* Pobrano 11.11.2012 z lokalizacji http://ed-thelen.org/comp-hist/NSA-Comb-p005b.jpg

Engelmann, M. (2007). Bezpieczeństwo informacji– Bezpieczeństwo fizyczne. *Boston IT Security Review No. 3*.

Esham, B. (2012). Pobrano 11.11.2012 z lokalizacji http://upload.wikimedia.org/wikipedia/commons/3/33/ROT13_table_with_example.svg

Fedirko, J. (2009). Einsteiniana. *Alma Mater nr 114* , s.80.

Fisher, B. (2000). *Przestępstwa komputerowe i ochrona informacji. Aspekty prawno – kryminalistyczne.* Kantor Wydawniczy Zakamycze.

Franksen, O. (1985). *Mr. Babbage's Secret: Tale of a Cipher-And APL.* Prentice Hall.

futurezone.at. (2012). Pobrano 11.11.2012 z lokalizacji http://futurezone.at/digitallife/8037-black-hat-die-lust-an-der-sicherheitsluecke.php

Gadomski, A. (2003). Socio-Cognitive Engineering Foundations and Applications: From Humans to Nations. *The Proceedings of SCEF2003, First International Workshop on Socio-Cognitive Engineering Foundations and Applications.* Rzym: Institute of Cognitive Sciences and Technologies.

Gagavai. (2012). *Myśli i aforyzmy – Gavagai.pl*. Pobrano 13.11.2012 z lokalizacji http://gavagai.pl

Garbarczuk, W. & Świć, A. (2005). *Podstawy ochrony informacji.* Lublin: Wydawnictwo Politechniki Lubelskiej.

Garfinkel, S. & Spafford, G. (1991). *Practical UNIX Security.* O'Reilly & Associates.

Garliński, J. (1999). *Enigma: tajemnica drugiej wojny światowej.* Lublin: Wydawnictwo Uniwersytetu Marii Curie-Skłodowskiej.

Grabowski, T. (2003). *Szyfrowanie na przyszłość.* Pobrano 11.11.2012 z lokalizacji http://obfusc.at/ed/cryptography_pl.html

Guzicki, W. (1997). Szyfry klasyczne. *Delta nr 4*.

Guzik, A. (2010). Ryzyko w bezpieczeństwie informacji. *Hakin9, nr 5*.

Hammond, N. (1973). *Dzieje Grecji.* Warszawa: Państwowy Instytut Wydawniczy.

Hatcher, T. (2001). *Survey: Costs of computer security breaches soar*. Pobrano 12.11.2012 z lokalizacji http://archives.cnn.com/2001/TECH/internet/03/12/csi.fbi.hacking.report/

Herodot. (1959). *Dzieje, ks. VIII.* Warszawa: Czytelnik.

iniejawna.pl. (2012). *Informacja Niejawna – Przeciwdziałanie zagrożeniom.* Pobrano 11.11.2012 z lokalizacji http://www.iniejawna.pl/pomoce/przeciw_zagr.html

Kaczmarek, A. (2012). *Wytyczne w zakresie opracowania i wdrożenia polityki bezpieczeństwa*. Pobrano 11.11.2012 z lokalizacji http://www.giodo.gov.pl/plik/id_p/778/j/pl/

Kahn, D. (2005). *Enigma. Złamanie kodu U-Bootów 1939-43.* Warszawa: Magnum.

Kahn, D. (1997). *The codebreakers: the comprehensive history of secret communication from ancient times to the Internet.* New York: Scribner's and Sons.

Kasiski, F. W. (1863). *Die Geheimschriften und die Dechiffrir-Kunst.* Berlin: E. S. Mittler und Sohn.

Kerckhoffs, A. (1883). La cryptographie militaire. *Journal des sciences militaires, vol. IX*, 5–83.

Kipper, G. (2003). *Investigator's Guide to Steganography.* Boca Raton: Auerbach Publications.

Knudsen, L. & Robshaw, M. (2011). *The Block Cipher Companion.* Springer.

Konieczny, P. (2012, 08 23). *TVP w Wiadomościach ujawniła (przypadkiem) hasło do systemu monitoringu śmigłowców ratowniczych*. Pobrano 14.11.2012 z lokalizacji http://niebezpiecznik.pl/post/wczoraj-w-wiadomosciach-tvp-ujawniono-hasla-do-systemow-ratowniczych/

kopalniawiedzy.pl. (2009). Pobrano 11.11.2012 z lokalizacji http://kopalniawiedzy.pl/dwustopniowe-uwierzytelnianie-haslo-jednorazowe-bank-wlamanie-two-factor-authentication,8555

KorpusPAN. (2012). *Korpus IPI PAN*. Pobrano 11.11.2012 z lokalizacji korpus.pl

Kozaczuk, W. (1984). *Enigma: How the German Machine Cipher Was Broken and How It Was Read by the Allies in World War Two.* Univ. Publications of America.

Large, C. (2003). *Hijacking Enigma: The Insider's Tale.* Wiley.

Laskowski, M. (2007). *Reorganizacja struktury sieci wewnętrznej Instytutu Informatyki Politechniki Lubelskiej (*praca mag.). Lublin: Politechnika Lubelska.

Laskowski, M. & Wilkołazki, S. (2005). Polityka bezpieczeństwa. W M. Miłosz, *Bezpieczeństwo informacji – od teorii do praktyki* (241-251). Warszawa: MIKOM.

Levy, S. (2001). *Crypto: How the Code Rebels Beat the Government — Saving Privacy in the Digital Age.*

Leyden, J. (2006, 04 19). *Mafia boss undone by clumsy crypto.* Pobrano 11.11.2012 z lokalizacji http://www.theregister.co.uk/2006/04/19/mafia_don_clueless_crypto/

Leyden, J. (2003, 04 18). *Office workers give away passwords for a cheap pen*. Pobrano 14.11.2012 z lokalizacji http://www.theregister.co.uk/2003/04/18/office_workers_give_away_passwords/

Long, J. (2008). *A Guide to Social Engineering, Dumpster Diving, and Shoulder Surfing.* Syngress.

Lubacz, J., Mazurczyk, W. & Szczypiorski, K. (2010, 4). Steganografia sieciowa. *Przegląd Telekomunikacyjny*, 134-135.

Luringen. (2012). Pobrano 11.11.2012 z lokalizacji http://upload.wikimedia.org/wikipedia/commons/5/51/Skytale.png

Łątka, J. (1985). *Carogrodzki pojedynek.* KAW.

Mason, S. (1991). *Secret Signals. The Euronumber Mistery.* Tiare Publications.

Merike, K. (2000). *Tworzenie bezpiecznych sieci.* Warszawa: MIKOM.

Mitnick, K. (2003). *Sztuka podstępu.* Helion.

Nadar, F. (2012). *Adam Jerzy Czartoryski by Felix Nadar.* Pobrano 11.11.2012 z lokalizacji http://austenetterespublica.wordpress.com/people/the-czartoryskis/izabela-czartoryska/adam-jerzy-czartoryski/adam-jerzy-czartoryski-by-nadar/

niebezpiecznik.pl. (2012). Pobrano 21.11.2012 z lokalizacji http://niebezpiecznik.pl/post/wojskowe-hasla-ujawnione-na-zdjeciach-ksiecia-wiliama/

niebezpiecznik.pl. (2011). *Hasło premiera Donalda Tuska.* Pobrano 11.11.2012 z lokalizacji http://niebezpiecznik.pl/post/haslo-premiera-donalda-tuska/

NIST. (1995). *An Introduction to Computer Security: The NIST Handbook.* NIST.

Nowik, G. (2004). *Zanim złamano Enigmę: Polski radiowywiad podczas wojny z bolszewicką Rosją, 1918–1920.*

NSA. (2012). Pobrano 11.11.2012 z lokalizacji http://www.nsa.gov/gallery/thumbs/thumb00050.jpg

Overbey, J., Traves, W. & Wojdylo, J. (2005). On the Keyspace of the Hill Cipher. *Cryptologia, Vol.29*, 59-72.

OxfordDictionary. (2012). *What is the frequency of the letters of the alphabet in English?* Pobrano 11.11.2012 z lokalizacji http://oxforddictionaries.com/words/what-is-the-frequency-of-the-letters-of-the-alphabet-in-english

Paterson, K. G. & Yau, A. K. (2006). Cryptography in theory and practice: The case of encryption in IPsec. *Lecture Notes in Computer Science*, 12-29.

pcgate.pl. (2012). Pobrano 1.11.2012 z lokalizacji http://www.pcgate.pl/readarticle.php?article_id=255

Piekałkiewicz, J. (1999). *Dzieje szpiegostwa.* Warszawa: Czytlenik.

Pieprzyk, J., Hardjono, T. & Seberry, J. (2006). *Teoria bezpieczeństwa systemów komputerowych.* Helion.

Piotrowski, M. (2008, 08 18). *Zarządzanie ryzykiem – cz. I* . Pobrano 11.11.2012 z lokalizacji http://www.e-ochronadanych.pl/a,297,zarzadzanie-ryzykiem-cz-i-.html

Poe, E. (2012). *Wybór opowiadań.* Świat Książki.

Polibiusz. (2005). *Dzieje.* Wrocław: Wydawnictwo Ossolineum/De Agostini.

Poltorak, A. (2012). *Mezuzah and Astrology.* Pobrano 11.11.2012 z lokalizacji http://www.chabad.org/library/article_cdo/aid/312102/jewish/Mezuzah-and-Astrology.htm

Poundstone, W. (1985). *Big secrets.* Harper Paperback.

Rejewski, M. (1980). An Application of the Theory of Permutations in Breaking the Enigma Cipher. *Applicationes Mathematicae 16*.

Rescorla, E. (2001). *SSL and TLS: Designing and Building Secure Systems.* Addison-Wesley .

Rivest, R., Shamir, A. & Adleman, L. (1978). A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. *Communications of the ACM 21 (2)*, 120-126.

Rosenheim, S. (1997). *The Cryptographic Imagination: Secret Writing from Edgar Poe to the Internet.* Baltimore: John Hopkins University Press.

Sacha, K., Cegieła, R. & Zalewski, A. (2012). *Instytucjonalizacja i standaryzacja audytu systemów informatycznych*. Pobrano 6.11. 2012 z lokalizacji http://www.e-informatyka.pl/article/show/481

Saltzer, J. & Schoeder, M. (1975). The protection of information in computer systems. *Proceedings of the IEEE 63(9)*, 1278 – 130.

Schneier, B. (2002). *Kryptografia dla praktyków: protokoły, algorytmy i programy źródłowe w języku C.* Warszawa: Wydawnictwa Naukowo-Techniczne.

Singh, S. (2003). *Księga szyfrów.* Warszawa: Świat Książki.

Słownik języka polskiego PWN. (2012). PWN.

Smith, M. (1998). *Station X: The Codebreakers of Bletchley Park.* London: Channel 4 Books/Macmilla.

Sokol, B. (2001, Luty 8). Espionage Is in the Air. *Miami New Times*.

SP12/193/54. [brak daty]. *The National Archives (United Kingdom).* Pobrano z lokalizacji http://www.nationalarchives.gov.uk/catalogue/searchresults.asp?SearchInit=4&SearchType=6&CATREF=SP12/193/54

SP53/18/55. [brak daty]. *The National Archives (United Kingdom).* Pobrano z lokalizacji http://www.nationalarchives.gov.uk/catalogue/searchresults.asp?SearchInit=4&SearchType=6&CATREF=SP12/193/54

Stallings, W. (1997). *Ochrona danych w sieci i intersieci.* Warszawa: WNT.

Starościak, G. (2004). *Algorytmy uwierzytelniania i szyfrowania przy egzaminowaniu przez Internet.* Gdańsk: Politechnika Gdańska.

Sun, T. (2008). *Sztuka wojny.* Helion.

sygma.pl. (2012). Pobrano 11.11.2012 z lokalizacji www.sygma.pl/index.php/sygma/oferta/wdrozenia_systemow_zarzadzania/system_zarzadzania_bezpieczenstwem_informacji_szbi

Szychowiak, M. (2012). *Wprowadzenie do problematyki bezpieczeństwa systemów komputerowych*. Pobrano 11.06.2012 z lokalizacji http://wazniak.mimuw.edu.pl/images/a/ae/Bsi_01_lab.pdf

Trankwillus, G. (1960). *Żywoty cezarów.* Wrocław.

United States v. Walter Kendall Myers. [brak daty]. Pobrano 11.11.2012 z lokalizacji http://i.cdn.turner.com/cnn/2009/images/06/05/myers.indictment.pdf

usc.edu. (2003). Pobrano 11.11.2012 z lokalizacji http://www.usc.edu/dept/molecular-science/RSA-2003.htm

White, W. (1992). *The Microdot: History and Application.* Williamstown: Phillips Publications.

Wielka Encyklopedia PWN. (2002). PWN.

Wobst, R. (2001). *Cryptology Unlocked.* Wiley.

Zwicky, E. D., Cooper, S. & Chapman, B. (2006). *Internet Firewalls – tworzenie zapór ogniowych.* Warszawa: Oficyna Wydawnicza READ ME.