helion.pl
KSIĘGARNIA INTERNETOWA · WYDAWNICTWO

IDŹ DO
PRZYKŁADOWY ROZDZIAŁ
SPIS TREŚCI

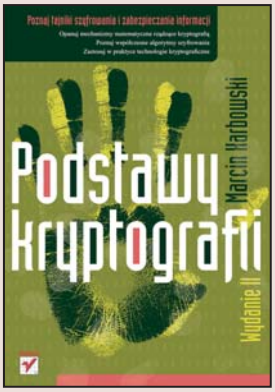
KATALOG KSIĄŻEK
KATALOG ONLINE
ZAMÓW DRUKOWANY KATALOG

TWÓJ KOSZYK
DODAJ DO KOSZYKA

CENNIK I INFORMACJE
ZAMÓW INFORMACJE O NOWOŚCIACH
ZAMÓW CENNIK

CZYTELNIA
FRAGMENTY KSIĄŻEK ONLINE

Podstawy kryptografii. Wydanie II



Autor: Marcin Karbowski
ISBN: 978-83-246-1215-4
Format: B5, stron: 304

Poznaj tajniki szyfrowania i zabezpieczania informacji

- Opanuj mechanizmy matematyczne rządzące kryptografią
- Poznaj współczesne algorytmy szyfrowania
- Zastosuj w praktyce technologie kryptograficzne

Większość z nas kojarzy szyfrowanie i kryptografię z filmami czy powieściami poświęconymi tajnym agentom wraz z ich zleceniodawcami. Tymczasem kryptografia – nauka znana od bardzo dawna i stosowana do przedstawiania określonych danych w formie zrozumiałej tylko dla wybranych osób – jest powszechnie wykorzystywana nie tylko w armii.

Dziś informacja stała się najcenniejszym towarem, a ochrona danych osobowych – niezwykle istotnym zagadnieniem. Dlatego efektywne sposoby zabezpieczania informacji mają żywotne znaczenie zarówno dla firm i instytucji, jak i osób prywatnych. Cyfrowe uwierzytelnianie poczty elektronicznej i witryn WWW czy łącza VPN to rozwiązania oparte o niezwykle złożone algorytmy kryptograficzne. Aby sprawnie korzystać z istniejących rozwiązań lub implementować własne, należy zapoznać się z podstawowymi wiadomościami związanymi z szyfrowaniem danych.

Książka „Podstawy kryptografii. Wydanie II" to doskonały przewodnik po wszelkich zagadnieniach dotyczących szyfrowania danych, uzupełniony o opisy najnowszych osiągnięć w tej dziedzinie. Znajdziesz tu wszystko, co jest niezbędne do zrozumienia i zastosowania zaawansowanych rozwiązań kryptograficznych. Poznasz historię kryptografii, aparat matematyczny leżący u podstaw tej nauki i teorię szyfrowania danych. Dowiesz się, jakie algorytmy szyfrowania stosowane są obecnie i do czego można je wykorzystać. Największy nacisk położono tu na stosowanie kryptografii w praktyce – czyli na opis protokołów SSL i SSH oraz kwestii związanych z podpisem elektronicznym, algorytmami PGP i implementacją szyfrowania danych w języku PHP.

- Historia kryptografii
- Matematyczne podstawy szyfrowania danych
- Szyfry strumieniowe, klucze publiczne i steganografia
- Zabezpieczanie połączeń internetowych
- Mechanizm PGP
- Certyfikaty cyfrowe i podpisy elektroniczne
- Protokoły SSL i SSH
- Najczęściej stosowane algorytmy szyfrujące

Zobacz, jak fascynująca jest kryptografia

Wydawnictwo Helion
ul. Kościuszki 1c
44-100 Gliwice
tel. 032 230 98 63
e-mail: helion@helion.pl

Spis treści

Kilka słów wstępu **9**

Rozdział 1. Historia kryptografii **13**
1.1. Prolog — Painvin ratuje Francję 13
1.2. Początek… 17
1.2.1. Steganografia 17
1.2.2. Kryptografia 18
1.2.3. Narodziny kryptoanalizy 20
1.3. Rozwój kryptografii i kryptoanalizy 21
1.3.1. Szyfry homofoniczne 21
1.3.2. Szyfry polialfabetyczne 22
1.3.3. Szyfry digraficzne 27
1.3.4. Kamienie milowe kryptografii 28
1.4. Kryptografia II wojny światowej 29
1.4.1. Enigma i Colossus 30
1.5. Era komputerów 35
1.5.1. DES 36
1.5.2. Narodziny kryptografii asymetrycznej 37
1.5.3. RSA 37
1.5.4. PGP 38
1.5.5. Ujawniona tajemnica 40
1.5.6. Upowszechnienie kryptografii 40

Rozdział 2. Matematyczne podstawy kryptografii **43**
2.1. Podstawowe pojęcia 44
2.1.1. Słownik tekstu jawnego 44
2.1.2. Przestrzeń tekstu 44
2.1.3. Iloczyn kartezjański 45
2.1.4. System kryptograficzny 46
2.1.5. Szyfrowanie monoalfabetyczne 47
2.1.6. Funkcje jednokierunkowe 47
2.1.7. Arytmetyka modulo 48
2.1.8. Dwójkowy system liczbowy 49
2.1.9. Liczby pierwsze 50
2.1.10. Logarytmy 54
2.1.11. Grupy, pierścienie i ciała 54
2.1.12. Izomorfizmy 56

2.2. Wzory w praktyce ... 57
2.2.1. Kryptosystem RSA ... 58
2.2.2. Problem faktoryzacji dużych liczb ... 60
2.2.3. Mocne liczby pierwsze ... 61
2.2.4. Generowanie liczb pierwszych ... 62
2.2.5. Chińskie twierdzenie o resztach ... 64
2.2.6. Logarytm dyskretny ... 65
2.2.7. XOR i AND ... 66
2.2.8. Testy zgodności ... 67
2.2.9. Złożoność algorytmów ... 76
2.2.10. Teoria informacji ... 77

Rozdział 3. Kryptografia w teorii ... 83
3.1. Ataki kryptoanalityczne i nie tylko ... 83
3.1.1. Metody kryptoanalityczne ... 83
3.1.2. Kryptoanaliza liniowa i różnicowa ... 85
3.1.3. Inne rodzaje ataków ... 87
3.2. Rodzaje i tryby szyfrowania ... 92
3.2.1. Szyfry blokowe ... 92
3.2.2. Szyfry strumieniowe ... 101
3.2.3. Szyfr blokowy czy strumieniowy? ... 106
3.3. Protokoły kryptograficzne ... 107
3.3.1. Protokoły wymiany kluczy ... 107
3.3.2. Podpis cyfrowy ... 111
3.3.3. Dzielenie sekretów ... 114
3.3.4. Inne protokoły ... 116
3.4. Infrastruktura klucza publicznego ... 120
3.4.1. PKI w teorii… ... 121
3.4.2. …i w praktyce ... 121
3.5. Kryptografia alternatywna ... 124
3.5.1. Fizyka kwantowa w kryptografii ... 124
3.5.2. Kryptografia DNA ... 130
3.5.3. Kryptografia wizualna ... 134
3.6. Współczesna steganografia ... 136
3.6.1. Znaki wodne ... 136
3.6.2. Oprogramowanie steganograficzne ... 138

Rozdział 4. Kryptografia w praktyce ... 141
4.1. Konstrukcja bezpiecznego systemu kryptograficznego ... 141
4.1.1. Wybór i implementacja kryptosystemu ... 142
4.1.2. Bezpieczny system kryptograficzny ... 143
4.1.3. Najsłabsze ogniwo ... 144
4.2. Zabezpieczanie połączeń internetowych ... 148
4.2.1. Protokół SSL ... 148
4.2.2. Protokół SSH ... 156
4.3. PGP ... 164
4.3.1. PGPkeys ... 164
4.3.2. PGPmail ... 167
4.3.3. PGPdisk ... 175
4.3.4. Standard PGP/MIME ... 182
4.3.5. Web of Trust ... 183
4.3.6. PGP 9.x ... 186

4.4. GnuPG ... 188
4.4.1. Generowanie klucza prywatnego ... 188
4.4.2. Obsługa programu ... 189
4.5. TrueCrypt ... 196
4.5.1. Tworzenie szyfrowanych dysków i partycji ... 197
4.5.2. Obsługa dysków wirtualnych ... 199
4.5.3. Ukryte dyski ... 200
4.5.4. Pozostałe opcje i polecenia ... 202
4.6. Składanie i weryfikacja podpisów elektronicznych ... 204
4.6.1. Wymagania techniczne ... 204
4.6.2. Jak zdobyć certyfikat cyfrowy? ... 206
4.6.3. O czym warto pamiętać? ... 209
4.6.4. Konfiguracja programu pocztowego ... 209
4.6.5. Struktura certyfikatu ... 215
4.7. Kryptografia w PHP i MySQL ... 217
4.7.1. Funkcje szyfrujące w PHP ... 217
4.7.2. Szyfrowanie danych w MySQL ... 222
4.7.3. Kolejne udoskonalenia ... 224

Podsumowanie ... 227

Dodatek A Jednokierunkowe funkcje skrótu ... 229

A.1. MD5 ... 229
A.1.1. Przekształcenia początkowe ... 229
A.1.2. Pętla główna MD5 ... 230
A.1.3. Obliczenia końcowe ... 232
A.2. SHA-1 ... 232
A.2.1. Przekształcenia początkowe ... 232
A.2.2. Pętla główna algorytmu SHA-1 ... 233
A.2.3. Operacje w cyklu SHA-1 ... 233
A.2.4. Obliczenia końcowe ... 234
A.3. SHA-2 ... 235
A.3.1. Dodatkowe pojęcia ... 235
A.3.2. Przekształcenia początkowe ... 236
A.3.3. Operacje w cyklu SHA-2 ... 237
A.3.4. Dodatkowe różnice między algorytmami SHA-2 ... 239
Inne funkcje skrótu ... 240

Dodatek B Algorytmy szyfrujące ... 241

B.1. IDEA ... 241
B.1.1. Przekształcenia początkowe ... 241
B.1.2. Operacje pojedynczego cyklu IDEA ... 241
B.1.3. Generowanie podkluczy ... 243
B.1.4. Przekształcenia MA ... 243
B.1.5. Deszyfrowanie IDEA ... 243
B.2. DES ... 245
B.2.1. Permutacja początkowa (IP) ... 245
B.2.2. Podział tekstu na bloki ... 245
B.2.3. Permutacja rozszerzona ... 247
B.2.4. S-bloki ... 248
B.2.5. P-bloki ... 249
B.2.6. Permutacja końcowa ... 250
B.2.7. Deszyfrowanie DES ... 250
B.2.8. Modyfikacje DES ... 251

B.3. AES ... 253
B.3.1. Opis algorytmu ... 253
B.3.2. Generowanie kluczy ... 253
B.3.3. Pojedyncza runda algorytmu ... 254
B.3.4. Podsumowanie ... 256
B.4. Twofish ... 256
B.4.1. Opis algorytmu ... 257
B.4.2. Pojedyncza runda algorytmu ... 257
B.4.3. Podsumowanie ... 261
B.5. CAST5 ... 262
B.5.1. Opis algorytmu ... 262
B.5.2. Rundy CAST5 ... 263
B.6. DSA ... 263
B.6.1. Podpisywanie wiadomości ... 264
B.6.2. Weryfikacja podpisu ... 264
B.6.3. Inne warianty DSA ... 265
B.7. RSA ... 266
B.7.1. Generowanie pary kluczy ... 266
B.7.2. Szyfrowanie i deszyfrowanie ... 266
B.8. Inne algorytmy szyfrujące ... 267

Dodatek C Kryptografia w służbie historii ... 269
C.1. Święte rysunki ... 270
C.1.1. 1000 lat później… ... 271
C.1.2. Szyfr faraonów ... 272
C.1.3. Ziarno przeznaczenia ... 273
C.1.4. Je tiens l'affaire! ... 274
C.1.5. Tajemnica hieroglifów ... 275
C.2. Język mitów ... 276
C.2.1. Mit, który okazał się prawdziwy ... 276
C.2.2. Trojaczki Kober ... 279
C.2.3. Raport z półwiecza ... 280
C.3. Inne języki ... 283

Bibliografia ... 285

Skorowidz ... 287

Rozdział 1.

Historia kryptografii

Dążenie do odkrywania tajemnic tkwi głęboko w naturze człowieka, a nadzieja dotarcia tam, dokąd inni nie dotarli, pociąga umysły najmniej nawet skłonne do dociekań. Niektórym udaje się znaleźć zajęcie polegające na rozwiązywaniu tajemnic… Ale większość z nas musi zadowolić się rozwiązywaniem zagadek ułożonych dla rozrywki: powieściami kryminalnymi i krzyżówkami. Odczytywaniem tajemniczych szyfrów pasjonują się nieliczne jednostki.

John Chadwick

Jeszcze nigdy tak wielu nie zawdzięczało tak wiele tak niewielu.

Winston Churchill

Szyfr Cezara wprowadzono w armii rosyjskiej w roku 1915, kiedy okazało się, że sztabowcom nie można powierzyć niczego bardziej skomplikowanego.

Friedrich L. Bauer

1.1. Prolog — Painvin ratuje Francję

21 marca 1918 roku o godzinie 4:30 rozpoczął się największy ostrzał artyleryjski I wojny światowej. Przez pięć godzin niemieckie działa pluły ogniem na pozycje połączonych sił brytyjskich i francuskich. Następnie 62 dywizje niemieckie zalały front na odcinku 60 kilometrów. Dzień po dniu alianci zmuszani byli do wycofywania się i dopiero tydzień później ofensywa została zatrzymana. Do tego czasu wojska niemieckie wbiły się 60 km poza linię frontu. Sukces ten wynikał w dużej mierze z przewagi liczebnej, jaką dysponowały — po kapitulacji Rosji przerzucono do Francji dywizje do tej pory związane walką na froncie wschodnim. Rozciągnięta linia frontu zmuszała obrońców do znacznego rozproszenia sił, co skwapliwie wykorzystywał generał Erich von Ludendorf. Jego taktyka opierała się na koncentrowaniu dużych sił w jednym punkcie i atakowaniu z zaskoczenia. Poznanie planów nieprzyjaciela było kluczowe dla skutecznej obrony. Dzięki temu możliwe stałoby się zgromadzenie większych sił na

zagrożonym odcinku frontu. Prowadzono więc intensywny nasłuch radiowy i przechwytywano liczne meldunki przesyłane między niemieckimi centrami dowodzenia, problem polegał jednak na tym, iż w większości wyglądały one mniej więcej tak:

> XAXXF AGXVF DXGGX FAFFA AGXFD XGAGX AVDFA GAXFX
> GAXGX AGXVF FGAXA…

Był to nowy szyfr stosowany przez niemieckie wojska. Nazwano go ADFGX od stosowanych liter alfabetu tajnego. Ich wybór nie był przypadkowy. W alfabecie Morse'a różniły się one w istotny sposób, dzięki czemu ewentualne zniekształcenia komunikatów radiowych były minimalne.

Jedynym sukcesem francuskiego wydziału szyfrów na tym etapie było złamanie innego niemieckiego systemu, tzw. Schlusselheft. Był to jednak szyfr stosowany głównie do komunikacji między oddziałami w okopach, natomiast naprawdę istotne informacje chronione były przy użyciu ADFGX. Wprowadzenie tego szyfru praktycznie oślepiło francuskie centrum dowodzenia. Najdobitniej świadczą o tym słowa ówczesnego szefa francuskiego wywiadu:

> „Z racji mego stanowiska jestem najlepiej poinformowanym człowiekiem we Francji, a w tej chwili nie mam pojęcia, gdzie są Niemcy. Jak nas dopadną za godzinę, nawet się nie zdziwię"[1].

Oczywiście Bureau du Chiffre nie pozostawało bezczynne. Zadanie złamania niemieckiego szyfru powierzono najlepszemu z francuskich kryptoanalityków — Georges'owi Painvinowi. Jednak nawet on nie był w stanie przeniknąć spowijającej ów szyfr tajemnicy. Zdołał jedynie ustalić, iż system oparty jest na szachownicy szyfrującej i że klucze zmienia się codziennie. Te informacje mogłyby się na coś przydać, gdyby przechwycono większą liczbę zaszyfrowanych depesz. Ta jednak była zbyt skromna i szyfr nadal pozostawał zagadką.

Sytuacja zmieniła się dopiero na początku kwietnia, kiedy Niemcy zwiększyli liczbę przekazów radiowych. W ręce Painvina wpadła większa ilość materiału do badań, co dało nadzieję na uczynienie pierwszych postępów w łamaniu szyfru. Po wstępnej analizie francuski kryptoanalityk zauważył, iż niektóre wiadomości pochodzące z tego samego dnia mają identyczne początki. Założył więc, że są to te same nagłówki meldunków zaszyfrowane kluczem dziennym. Pozwoliło mu to wydobyć pierwsze informacje na temat konstruowania tego klucza. Następnie posegregował wiadomości na segmenty o takich samych początkach i przesuwając je względem siebie, próbował znaleźć kolejne prawidłowości. Ogromnie pomocne okazało się przechwycenie 18 wiadomości tego samego dnia. Wszystkie były zaszyfrowane tym samym kluczem, dzięki czemu Painvin był w stanie porównać je ze sobą i wyodrębnić stosowane do szyfrowania pary liter (AA, AD, AF itd.). Następnie policzył częstotliwość występowania poszczególnych par. Najczęściej pojawiała się kombinacja DG. Nasunęło mu to podejrzenie, iż odpowiadała ona literze e, najczęściej pojawiającej się w języku niemieckim. Udało mu się również ustalić wygląd stosowanej tablicy (rysunek 1.1).

[1] Kahn D., *Łamacze kodów — historia kryptologii*, Wydawnictwa Naukowo-Techniczne, Warszawa 2004.

Rysunek 1.1. *Tablica podstawień szyfru ADFGX ustalona przez Painvina*

	A	D	F	G	X
A					
D				e	
F					
G					
X					

Na niemieckim systemie szyfrowania pojawiła się pierwsza rysa. Był to jednak dopiero początek drogi. Teraz należało ustalić współrzędne pozostałych liter. Rozpoczęły się długie dni mozolnej analizy statystycznej przechwyconych kryptogramów. Painvin porównywał częstotliwość występowania pojedynczych liter w parach i na tej podstawie dzielił kryptogramy. Przypisał każdej literze dwie współrzędne — górną i boczną — a następnie próbował je ustalić. Opierał się na każdym, najmniejszym nawet strzępku informacji, jaki udało mu się zdobyć: na częstości występowania czy parzystości lub nieparzystości sumy współrzędnych. Mozolnie, litera po literze, zrekonstruował niemiecką tabelę podstawień i był teraz w stanie rekonstruować dzienne klucze niemieckich szyfrantów. Przed końcem maja doszedł do takiej wprawy, iż otrzymane wiadomości był w stanie odczytać już po dwóch dniach. I wtedy stało się to, czego najbardziej się obawiał. Niemcy zmienili szyfr.

Komunikaty niemieckie przechwycone 1 czerwca zawierały dodatkową literę — *V*. Oznaczało to zmianę wyglądu tabeli szyfrowania i być może całego systemu. Tymczasem niemiecka ofensywa trwała. Decydujący atak był kwestią czasu, a Francuzi stracili właśnie możliwość przewidzenia, w którym miejscu nastąpi. Po długiej, bezsennej nocy i kolejnym dniu pracy Painvinowi udało się jednak, poprzez porównywanie starych i nowych kryptogramów, odtworzyć szachownicę szyfrowania (rysunek 1.2).

Rysunek 1.2. *Tablica szyfru ADFGVX*

	A	D	F	G	V	X
A	c	o	8	x	f	4
D	m	k	3	a	z	9
F	n	w	1	0	j	d
G	5	s	i	y	h	u
V	p	1	v	b	6	r
X	e	q	7	t	2	g

Czym prędzej zabrał się do łamania przechwyconych wiadomości i już tego samego dnia udało mu się wysłać pierwsze cenne informacje do sztabu dowodzenia. Mniej więcej w tym samym czasie pierwsze pociski z niemieckich dział dalekosiężnych spadły na Paryż…

Czasu było coraz mniej. Linia frontu była zbyt długa, by należycie zabezpieczyć wszelkie możliwe punkty ataku. Należało więc za wszelką cenę zdobyć informację, gdzie Ludendorf zamierza uderzyć. Francuzi wzmocnili nasłuch radiowy i czekali. 3 czerwca udało się przechwycić depeszę z niewielkiego miasteczka Remaugies, opanowanego

przez wojska niemieckie. Po jej odczytaniu okazało się, iż zawiera ona rozkaz przysłania dużej ilości amunicji. To mogło być to! Ciężki ostrzał artyleryjski przed rozpoczęciem szturmu był powszechną praktyką. Zwiad lotniczy istotnie zaobserwował w ciągu kolejnych dni dużą liczbę ciężarówek na drogach prowadzących do Remaugies. Hipotezę o ataku potwierdzały również informacje od schwytanych jeńców i dezerterów. Prawdopodobną datę ataku wyznaczono na 7 czerwca.

Nie pozostawało już nic innego, jak tylko wzmocnić odpowiedni odcinek frontu i czekać. Wzmocniono obie linie obrony i poinformowano oficerów o zbliżającym się natarciu. Wreszcie nadszedł decydujący dzień. W nerwowym oczekiwaniu żołnierze spoglądali w kierunku niemieckich umocnień. Nic się jednak nie działo. Tak upłynął 7 czerwca, a po nim 8. Napięcie rosło. Oczywiście możliwe było pewne opóźnienie ataku, a informacje od jeńców mogły być nieścisłe, a jednak… w serca obrońców wkradł się niepokój. Wreszcie o północy 9 czerwca niemieckie działa otworzyły ogień. Francuskie linie były bombardowane przez 3 godziny z niespotykaną dotąd intensywnością. Chwilę później nastąpił atak.

Do przodu ruszyło 15 niemieckich dywizji. Kolejnych pięć dni wypełnionych było ciągłą walką o każde miasteczko i ulicę. Niemcy postępowali naprzód, by kolejnego dnia ustępować przed kontratakiem Francuzów. Jeśli jednak ktokolwiek był zaskoczony przebiegiem bitwy, to jedynie generał von Ludendorf. Po raz pierwszy nie udało mu się skoncentrowanym atakiem przełamać linii oporu wroga. Co więcej, wróg odważnie kontratakował. W ciągu następnych tygodni próbował jeszcze kolejnych ataków, jednak wkrótce zabrakło mu sił. Paryż został ocalony. A wraz z nim Francja.

Wkrótce potem w Europie wylądowały siły amerykańskie. Dzięki ich wsparciu alianci byli w stanie przystąpić do kontrofensywy, zmuszając Niemców do odwrotu i ostatecznie do poddania się. Niemieccy generałowie podpisali akt kapitulacji 11 października w miejscowości Compiegne. I wojna światowa została zakończona. A Painvin? Cóż… Painvin pojechał na zasłużony urlop. Po latach, zapytany o historię złamania szyfru ADFGVX, odpowiedział:

> „Osiągnięcie to pozostawiło niezmywalny ślad na mej duszy i pozostało jednym z najjaśniejszych i najwspanialszych wspomnień w całym moim życiu”[2].

I trudno mu się chyba dziwić. Nie każdemu dane jest ocalić własny kraj.

Przytoczona tu historia stanowi niewątpliwie znakomity materiał na film. Wiele osób może zadziwić to, jak wielki wpływ na losy wojny może mieć jeden człowiek. Oczywiście bez odpowiedniej reakcji ze strony dowództwa, odpowiedniego planowania i wykorzystywania zdobytej przewagi, a przede wszystkim bez odwagi i poświęcenia zwykłych żołnierzy, którzy oddali życie za swój kraj, informacje zdobyte przez Painvina zostałyby zmarnowane. Z drugiej jednak strony, gdyby nie on, szanse na ocalenie Paryża byłyby nikłe. Upadek stolicy wpłynąłby zaś nie tylko na losy Francji, ale i na wynik całej wojny.

[2] Kahn D., *Łamacze kodów — historia kryptologii*, op.cit.

Tymczasem z punktu widzenia historii kryptografii przypadek francuskiego kryptoanalityka nie jest niczym niezwykłym. Historia ta jest pełna opowieści o jemu podobnych, którzy, łamiąc szyfr, decydowali o losach setek, tysięcy lub nawet milionów ludzi. Jednak ich osiągnięcia często wychodziły na jaw dopiero po latach, kiedy tajemnice rządowe mogły zostać bezpiecznie ujawnione. Byli więc szarymi eminencjami historii, wpływali na bieg politycznych negocjacji, gry wywiadów czy wreszcie wojen. Wszystko dzięki znakomitemu opanowaniu sztuki „sekretnego pisma" pozwalającej na odkrywanie cudzych tajemnic i zabezpieczanie swoich. Historia kryptografii to opowieść o tych właśnie ludziach. A zatem posłuchajcie…

1.2. Początek…

Na początku było pismo. Wykształcone niezależnie w wielu kulturach stanowiło niezbadaną tajemnicę dla tych, którzy nie potrafili czytać. Szybko jednak zrodziła się konieczność ukrycia informacji również przed tymi, którym umiejętność ta nie była obca. Najbardziej oczywistym rozwiązaniem było schowanie tajnej wiadomości przed ludźmi, którzy mogliby ją odczytać. Takie zabiegi wkrótce jednak przestały wystarczać. Wiadomość mogła zostać odnaleziona podczas wnikliwego przeszukania, a wtedy tajne informacje dostałyby się w ręce wroga. A gdyby udało się napisać list działający na zasadzie „drugiego dna"? Z pozoru zawierałby on błahe treści, jednak jeśli adresat wiedziałby, gdzie i jak szukać, mógłby dotrzeć do „mniej niewinnych" informacji. Tak narodziła się steganografia.

1.2.1. Steganografia

Steganografia to ogół metod ukrywania tajnych przekazów w wiadomościach, które nie są tajne. Jej nazwa wywodzi się od greckich słów: *steganos* (ukryty) oraz *graphein* (pisać). W przeszłości stosowano wiele wymyślnych sposobów osiągnięcia tego efektu. Popularny niewidzialny atrament to jeden z najbardziej znanych przykładów steganografii. Pierwsze zapiski na temat stosowania tej sztuki znaleźć można już w księgach z V wieku p.n.e. Przykładem może być opisana przez Herodota historia Demaratosa, Greka, który ostrzegł Spartan przed przygotowywaną przeciw nim ofensywą wojsk perskich. Nie mógł on wysłać oficjalnej wiadomości do króla, zeskrobał więc wosk z tabliczki i wyrył tekst w drewnie. Następnie ponownie pokrył tabliczkę woskiem i wręczył posłańcowi. Czysta tabliczka nie wzbudziła podejrzeń perskich patroli i bezpiecznie dotarła do celu. Tam, co prawda, długo głowiono się nad jej znaczeniem, wkrótce jednak żona spartańskiego wodza Leonidasa wpadła na pomysł zeskrobania wosku, co pozwoliło odkryć tajną wiadomość.

W miarę postępu technicznego, a także rozwoju samej steganografii, powstawały coraz wymyślniejsze metody ukrywania wiadomości. Znana jest na przykład metoda ukrywania wiadomości w formie kropki w tekście drukowanym, stosowana podczas II wojny światowej. Wiadomość była fotografowana, a klisza pomniejszana do rozmiarów około mm^2 i naklejana zamiast kropki na końcu jednego ze zdań w liście. Obecnie

bardzo popularne jest ukrywanie wiadomości w plikach graficznych. Kolejne przykłady można mnożyć, jednak nawet najbardziej wymyślne z nich nie gwarantują, iż wiadomość nie zostanie odkryta. Koniecznością stało się zatem wynalezienie takiego sposobu jej zapisywania, który gwarantowałby tajność nawet w przypadku przechwycenia przez osoby trzecie.

1.2.2. Kryptografia

Nazwa *kryptografia* również wywodzi się z języka greckiego (od wyrazów *kryptos* — ukryty i *graphein* — pisać). Jej celem jest utajnienie znaczenia wiadomości, a nie samego faktu jej istnienia. Podobnie jak w przypadku steganografii, data jej powstania jest trudna do określenia. Najstarsze znane przykłady przekształcenia pisma w formę trudniejszą do odczytania pochodzą ze starożytnego Egiptu, z okresu około 1900 roku p.n.e. Pierwsze tego typu zapisy nie służyły jednak ukrywaniu treści przed osobami postronnymi, a jedynie nadaniu napisom formy bardziej ozdobnej lub zagadkowej. Skrybowie zapisujący na ścianach grobowców historie swych zmarłych panów świadomie zmieniali niektóre hieroglify, nadając napisom bardziej wzniosłą formę. Często celowo zacierali ich sens, zachęcając czytającego do rozwiązania zagadki. Ten element tajemnicy był ważny z punktu widzenia religii. Skłaniał on ludzi do odczytywania epitafium i tym samym do przekazania błogosławieństwa zmarłemu. Nie była to kryptografia w ścisłym tego słowa znaczeniu, zawierała jednak dwa podstawowe dla tej nauki elementy — przekształcenie tekstu oraz tajemnicę.

Na przestrzeni kolejnych 3000 lat rozwój kryptografii był powolny i dosyć nierówny. Powstawała ona niezależnie w wielu kręgach kulturowych, przybierając różne formy i stopnie zaawansowania. Zapiski na temat stosowania szyfrów znaleziono na pochodzących z Mezopotamii tabliczkach z pismem klinowym. Ich powstanie datuje się na 1500 rok p.n.e. W II w. p.n.e. grecki historyk Polibiusz opracował system szyfrowania oparty na tablicy przyporządkowującej każdej literze parę cyfr (rysunek 1.3).

Rysunek 1.3. *Tablica Polibiusza*

	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

W późniejszych czasach tablica ta stała się podstawą wielu systemów szyfrowania. Przekształcenie liter w liczby dawało możliwość wykonywania dalszych przekształceń za pomocą prostych obliczeń lub funkcji matematycznych. Metodę Polibiusza uzupełnioną kilkoma dodatkowymi utrudnieniami kryptoanalitycznymi zastosowała m.in. niemiecka armia przy opracowywaniu wspomnianego na wstępie systemu szyfrującego ADFGX oraz jego udoskonalonej wersji ADFGVX.

Pierwsze wzmianki dotyczące stosowania kryptografii w celach politycznych pochodzą z IV w. p.n.e. z Indii. Wymieniana jest ona jako jeden ze sposobów zdobywania informacji przez przebywających za granicą ambasadorów. Sekretne pismo wspomniane jest również w słynnej *Kamasutrze* — figuruje tam jako jedna z 64 sztuk, które kobieta powinna znać.

Ogólnie stosowane w starożytności metody kryptografii można podzielić na dwa rodzaje — przestawianie i podstawianie. W pierwszym przypadku następowała zamiana szyku liter w zdaniach, czyli, innymi słowy, tworzony był anagram. Przykładem szyfrowania przestawieniowego jest pierwsze znane urządzenie szyfrujące — spartańska ***scytale*** z V w. p.n.e. Miała ona kształt pręta o podstawie wielokąta, na który nadawca nawijał skórzany pas. Wiadomość pisana była wzdłuż pręta, po czym odwijano pas, na którym widać było tylko pozornie bezsensowną sekwencję liter. Potem goniec przenosił list do adresata, stosując czasem steganograficzne sztuczki, na przykład opasując się nim i ukrywając tekst po wewnętrznej stronie. Odczytanie wiadomości było możliwe przy użyciu scytale o takiej samej grubości, jaką miał pręt nadawcy.

Druga, bardziej popularna metoda polegała na podstawianiu za litery tekstu jawnego innych liter bądź symboli. Za przykład może tu posłużyć szyfr Cezara, najsłynniejszy algorytm szyfrujący czasów starożytnych (jego twórcą był Juliusz Cezar). Szyfr ten opierał się na zastąpieniu każdej litery inną, położoną o trzy miejsca dalej w alfabecie. W ten sposób na przykład wiadomość o treści *Cesar* przekształca się w *Fhvdu*. Adresat znający sposób szyfrowania w celu odczytania wiadomości zastępował każdą literę tekstu tajnego literą położoną o trzy miejsca wcześniej w alfabecie (rysunek 1.4).

Rysunek 1.4. *Szyfr Cezara*

Alfabet jawny –	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
	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓
Alfabet tajny –	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

Szyfry przyporządkowujące każdej literze alfabetu jawnego dokładnie jedną literę, kombinację cyfr lub symbol nazywamy szyframi monoalfabetycznymi. W przypadku szyfru Cezara układ alfabetu tajnego zawsze pozostawał ten sam. Znacznie bezpieczniejszym rozwiązaniem było dokonywanie w nim okresowych zmian tak, aby znajomość metody szyfrowania nie wystarczała do odczytania wiadomości.

Stanowiło to jednak utrudnienie również dla adresata. Musiał on dodatkowo posiadać klucz (układ liter lub symboli w alfabecie tajnym). Tak powstał największy problem w historii kryptografii — dystrybucja klucza. Raz przechwycony klucz stawał się bezużyteczny, gdyż wiadomości szyfrowane za jego pomocą nie były już bezpieczne. O ile w przypadku wymiany wiadomości między dwiema osobami nie była to z reguły duża przeszkoda (wystarczyło ustalić nowy klucz), o tyle w przypadku szyfrowania na potrzeby wojskowe rodziło to bardzo wiele problemów. Trzeba było dostarczyć nowy klucz do wszystkich jednostek i to możliwie szybko, gdyż każda przechwycona przez wroga wiadomość stawała się dla niego łatwa do odczytania.

1.2.3. Narodziny kryptoanalizy

Kolebką kryptoanalizy były państwa arabskie, które najlepiej opanowały sztukę lingwistyki i statystyki, na nich bowiem opierała się technika łamania szyfrów monoalfabetycznych. Najwcześniejszy jej opis znajduje się w pracy Al-Kindiego, uczonego z IX wieku, znanego jako „filozof Arabów" (napisał on 29 prac z dziedziny medycyny, astronomii, matematyki, lingwistyki i muzyki). Jego największy traktat, *O odczytywaniu zaszyfrowanych listów*, został odnaleziony w 1987 roku w Archiwum Ottomańskim w Stambule. W pracy tej Al-Kindi zawarł szczegółowe rozważania na temat statystyki fonetyki i składni języka arabskiego oraz opis opracowanej przez siebie techniki poznawania tajnego pisma. To jeden z pierwszych udokumentowanych przypadków zastosowania ataku kryptoanalitycznego. Pomysł arabskiego uczonego był następujący:

> „Jeden sposób na odczytanie zaszyfrowanej wiadomości, gdy wiemy, w jakim języku została napisana, polega na znalezieniu innego tekstu w tym języku, na tyle długiego, by zajął mniej więcej jedna stronę, i obliczeniu, ile razy występuje w nim każda litera. Literę, która występuje najczęściej, będziemy nazywać »pierwszą«, następną pod względem częstości występowania »drugą« i tak dalej, aż wyczerpiemy listę wszystkich liter w próbce jawnego tekstu.

Następnie bierzemy tekst zaszyfrowany i również klasyfikujemy użyte w nim symbole. Znajdujemy najczęściej występujący symbol i zastępujemy go wszędzie „pierwszą" literą z próbki jawnego tekstu. Drugi najczęściej występujący symbol zastępujemy „drugą" literą, następny „trzecią" i tak dalej, aż wreszcie zastąpimy wszystkie symbole w zaszyfrowanej wiadomości, którą chcemy odczytać"[3].

Opisana powyżej metoda znana jest jako analiza częstości i po dziś dzień stanowi podstawową technikę kryptoanalityczną. Każdy język posiada własną charakterystykę występowania poszczególnych liter w piśmie, zawsze jednak pewne znaki pojawiają się częściej niż inne. Na tej podstawie kryptoanalityk może zidentyfikować te litery w kryptogramie. To z kolei pozwala odgadnąć niektóre ze znajdujących się w tajnym piśmie wyrazów, dzięki czemu rozszyfrowuje się kolejne litery itd. Wszystko opiera się tutaj w dużej mierze na prawdopodobieństwie, gdyż najczęściej występujący w kryptogramie znak wcale nie musi być literą najczęściej występującą w danym języku. Niemniej jednak znajomość tej metody pozwalała znacznie zredukować liczbę możliwych podstawień i osiągnąć rozwiązanie metodą prób i błędów.

Należy tu podkreślić, że jeśli mamy do czynienia z jedną krótką wiadomością, analiza częstości występowania znaków może dać fałszywe wyniki (w tych kilku konkretnych zdaniach najczęściej pojawiającą się literą może być na przykład czternasta pod względem częstości występowania w danym języku) i utrudnić dekryptaż. **Stąd też im dłuższy jest zaszyfrowany tekst, tym większa szansa na złamanie szyfru**.

Dzięki wynalazkowi Al-Kindiego monoalfabetyczne systemy szyfrujące przestały być bezpieczne. Od tej chwili rozpoczął się trwający do dziś wyścig kryptografów z kryptoanalitykami.

---

[3] Singh S., *Księga szyfrów*, Albatros, Warszawa 2001, s. 31.

1.3. Rozwój kryptografii i kryptoanalizy

Jeszcze wiele lat po odkryciu Al-Kindiego liczni uczeni negowali możliwość złamania szyfru podstawieniowego. Szybko jednak metody kryptoanalityczne rozprzestrzeniły się z Bliskiego Wschodu na Europę. W średniowieczu nie dokonał się większy postęp w europejskiej kryptologii. Szyfry znane były mnichom i skrybom, a i ci nie traktowali ich jako odrębnej nauki, a jedynie jako rodzaj intelektualnej rozrywki. Aż do początków XV wieku używano wyłącznie szyfrów podstawieniowych. Popularne były również tzw. ***nomenklatory***. Było to połączenie szyfru podstawieniowego z kodem — oprócz klasycznego alfabetu tajnego nomenklator zawierał listę słów i ich odpowiedników kodowych. Prawdziwy rozkwit technik szyfrowania nastąpił równolegle z rozwojem i umacnianiem stosunków dyplomatycznych między europejskimi państwami. Ambasadorowie, pełniący jednocześnie rolę szpiegów na obcych dworach, potrzebowali sposobu na bezpieczne przekazywanie tajnych informacji. Z tych samych powodów wzrosło zainteresowanie kryptoanalizą. W związku z dokonanymi w tej dziedzinie postępami szyfry monoalfabetyczne nie były już bezpieczne, zaczęto więc opracowywać nowe metody szyfrowania.

1.3.1. Szyfry homofoniczne

Jedną z najbardziej znanych metod jest szyfrowanie z użyciem homofonów. Miało ono zabezpieczyć szyfr przed atakiem z użyciem analizy częstości. Pierwszy znany przykład szyfru homofonicznego pochodzi z roku 1401. W szyfrach takich alfabet tekstu tajnego wzbogacano o pewne dodatkowe symbole, które następnie przypisywano najczęściej występującym w alfabecie tekstu jawnego literom. I tak, jeśli częstość występowania danej litery wynosiła 7%, przypisywano jej 7 różnych symboli. W ten sposób każdy znak tekstu tajnego pojawiał się w wiadomości z taką samą częstością. Mogłoby się wydawać, że od tej chwili tajne wiadomości pozostaną nieodczytane. Nic bardziej mylnego.

Częstość występowania liter nie jest jedyną charakterystyką języka. Istnieją również liczne powiązania między literami, takie jak częstość pojawiania się określonych par i trójek. Poszczególne wyrazy w języku również charakteryzują się określoną częstotliwością występowania. Dzięki takim prawidłowościom możliwa jest kryptoanaliza szyfrów homofonicznych poprzez wyszukiwanie tzw. częściowych powtórzeń. Załóżmy dla przykładu, iż szyfrowanie opiera się na podstawianiu par cyfr zamiast liter. Literom o większej częstości występowania przypisana jest większa liczba kombinacji dwucyfrowych. Tak skonstruowany szyfr można złamać przy odpowiedniej ilości materiału do badań. Wystarczy wyszukać w tekście podobne kombinacje znaków, na przykład: 67 55 10 23 i 67 09 10 23. Z dużą dozą prawdopodobieństwa założyć można, iż odpowiadają one tym samym wyrazom. Dzięki temu łatwo zidentyfikować zestawy cyfr odpowiadające tej samej literze (w naszym przykładzie — 55 i 09). Po odtworzeniu odpowiedniej liczby takich powiązań szyfr złamać można tradycyjną metodą analizy częstości. Zaczęto więc udoskonalać szyfry homofoniczne, aby uodpornić je na tego typu kryptoanalizę.

Bardzo wiele usprawnień w szyfrowaniu wprowadziła włoska rodzina Argentich. W XVI i XVII wieku jej członkowie pracowali dla kolejnych papieży, służąc im swoją bogatą wiedzą kryptologiczną. Na początku XVII wieku wprowadzili liczne udoskonalenia w stosowanych wówczas technikach szyfrowania.

Przede wszystkim stosowali symbole puste w każdym wierszu kryptogramu. Zlikwidowali również rozdzielanie wyrazów i zapisywanie znaków interpunkcyjnych. Nawet cyfry odpowiadające poszczególnym literom zapisywali razem, mieszając często liczby jedno- i dwucyfrowe. Dzięki tym zabiegom problem pojawiał się już na etapie podziału tekstu tajnego na pojedyncze znaki. Oczywiście, złamanie szyfru nadal było możliwe, jednak zadanie to było znacznie trudniejsze niż w przypadku zwykłego szyfru homofonicznego.



Symbol pusty — znak alfabetu tajnego nieposiadający odpowiednika w alfabecie jawnym. Adresat wiadomości podczas dekryptażu ignoruje takie znaki, natomiast dla kryptoanalityka są one dodatkowym utrudnieniem.

1.3.2. Szyfry polialfabetyczne

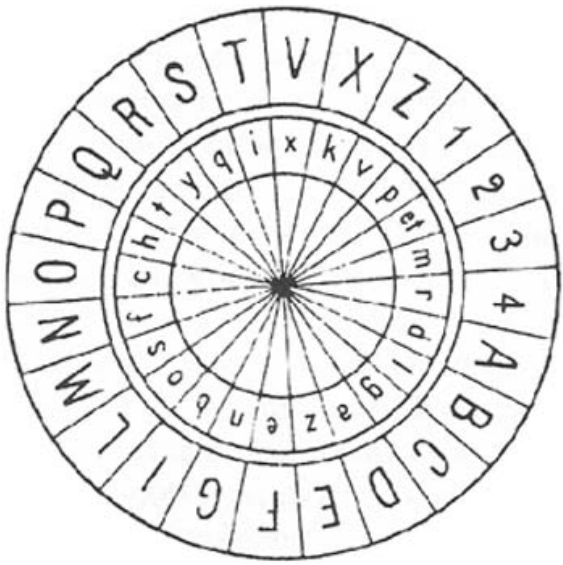
Szyfry polialfabetyczne opisać można jako połączenie wielu szyfrów monoalfabetycznych. Mają wiele alfabetów tajnych, z których każdy szyfruje jeden znak tekstu tajnego. Używane są cyklicznie, a więc po wyczerpaniu wszystkich powraca się do pierwszego i kontynuuje szyfrowanie. Prawdopodobnie pierwszym zastosowanym szyfrem polialfabetycznym był szyfr Albertiego, włoskiego architekta z XV wieku.

1.3.2.1. Tarcza Albertiego

Urodzony w roku 1404 Leone Battista Alberti był człowiekiem niezwykle wszechstronnym — komponował, malował, pisał, zajmował się aktorstwem, architekturą, prawem. Kryptografią zainteresował się dosyć późno, bo dopiero w roku 1466, za namową Leonardo Dato — ówczesnego papieskiego sekretarza.

Alberti napisał obszerną rozprawę o tematyce kryptologicznej. Obejmowała ona zarówno zagadnienia kryptoanalizy, jak i metodologii tworzenia nowych szyfrów. Architekt opisał w niej również swój własny szyfr i stwierdził, iż nikt nie będzie w stanie go złamać. Szyfr ten opierał się na urządzeniu zaprojektowanym przez niego samego. Składało się ono z dwóch okrągłych tarcz (rysunek 1.5).

Jedna z nich zawierała się wewnątrz drugiej, na obu zaś, na osobnych polach, wypisane były litery alfabetu. Szyfrowanie polegało na zastępowaniu liter z małej tarczy literami znajdującymi się na odpowiadających im polach dużej. Wszystko to tworzyłoby jedynie prosty szyfr monoalfabetyczny, gdyby nie fakt, iż wewnętrzna tarcza była ruchoma. Obracając ją, szyfrujący zmieniał przypisania wszystkich używanych liter, tym samym wybierając nowy alfabet szyfrowy. Oczywiście osoby prowadzące zaszyfrowaną korespondencję przy użyciu tarczy Albertiego muszą posiadać jej identyczne egzemplarze i ustalić początkową pozycję wewnętrznej tarczy względem zewnętrznej.



Rysunek 1.5.
Tarcza Albertiego

Źródło: Kahn D., Łamacze kodów — historia kryptologii, op.cit.

Dodatkowo włoski architekt umieścił na zewnętrznej tarczy cyfry od 1 do 4, co umożliwiało wstawianie do wiadomości słów kodowych (na przykład nazwy własne mogły być zastępowane kombinacjami cyfr). W połączeniu z wynalezieniem szyfru polialfabetycznego i dokonaniem pierwszego na Zachodzie opisu kryptoanalizy stanowiło to niebywałe osiągnięcie, zwłaszcza jak na człowieka, który kryptografią zajmował się raptem kilka lat. Osiągnięcia Albertiego zyskały mu miano *ojca kryptologii Zachodu*.

Szyfrowanie z użyciem wielu alfabetów stanowiło wielki przełom, jednak stosowanie w tym celu urządzenia szyfrującego powodowało pewne niedogodności. Pół wieku później zupełnie inny sposób wykorzystania techniki szyfrowania polialfabetycznego zaproponował niemiecki uczony Johannes Trithemius.

1.3.2.2. Tabula recta

Trithemius urodził się 2 lutego 1462 roku w Trittenheim w Niemczech. W wieku 17 lat rozpoczął studia na uniwersytecie w Heidelbergu, gdzie szybko zdobył uznanie dzięki swemu niebywałemu intelektowi. Mając lat dwadzieścia, przez przypadek trafił do opactwa benedyktynów. Życie mnichów zafascynowało go do tego stopnia, iż postanowił rozpocząć nowicjat. Niecałe dwa lata później wybrany został opatem.

Oprócz sprawowania swego nowego stanowiska Trithemius zajmował się pisaniem książek. Pierwsza z nich została opublikowana, kiedy miał 24 lata. Pisał opowieści, słowniki, biografie, kroniki oraz kazania. Prowadził też bogatą korespondencję z innymi uczonymi. W roku 1499 rozpoczął pisanie książki pt. *Steganographia*. Opisywała ona znane metody szyfrowania. Tak naprawdę jednak w książce tej więcej było okultyzmu i czarnej magii niż kryptografii. Trithemius nie ukrywał swej fascynacji praktykami magicznymi i lubił uchodzić za cudotwórcę. Ze zrozumiałych względów kościelni zwierzchnicy zdecydowanie potępiali postępowanie opata i ostatecznie nie ukończył on swojej książki.

W roku 1508 Trithemius powrócił do tematyki kryptologicznej, tym razem traktując temat bardziej naukowo. Jego kolejna książka — *Poligraphia* — skupiała się wyłącznie na zagadnieniach czysto kryptograficznych. Ukazała się ona dopiero w roku 1518, dwa lata po śmierci uczonego. Była to pierwsza książka na temat kryptologii wydana drukiem. Jej tytuł brzmiał: *Sześć ksiąg o poligrafii przez Johannesa Trithemiusa, opata w Wurzburgu, poprzednio w Spanheim, dla cesarza Maksymiliana*. Książka zawierała głównie kolumny słów używanych przez Trithemiusa w jego systemach kryptograficznych. W księdze piątej znajdował się jednak opis nowego systemu szyfrowania polialfabetycznego. Opierał się on na specjalnej tabeli nazwanej przez Trithemiusa *tabula recta*. Przedstawia ją rysunek 1.6.

Rysunek 1.6.
Tabela Trithemiusa

	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
1.	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
2.	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
3.	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
4.	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
5.	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
6.	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
7.	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
8.	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
9.	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
10.	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
11.	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
12.	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
13.	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
14.	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
15.	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
16.	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
17.	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
18.	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
19.	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
20.	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
21.	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
22.	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
23.	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
24.	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
25.	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
26.	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

Na samej górze tabeli umieszczono alfabet tekstu tajnego. Kolejne linijki to tajne alfabety utworzone przez przenoszenie kolejnych liter z początku alfabetu na jego koniec. W ten sposób Trithemius uzyskał 26 alfabetów szyfrowych.

Szyfrowanie tą metodą przebiega następująco: dla pierwszej litery tekstu jawnego używa się pierwszej linijki tabeli, dla drugiej litery — drugiej linijki itd. Pozwala to na zabezpieczenie tekstu przed atakiem przez analizę częstości. Jednak, podobnie jak w przypadku szyfru Cezara, nie chroni to przed odszyfrowaniem w przypadku, gdy kryptoanalityk zna stosowany algorytm. Próbą rozwiązania tego problemu był opublikowany w 1586 roku szyfr Vigenere'a.

1.3.2.3. Le chiffre indechiffrable

Blaise de Vigenere urodził się 5 kwietnia 1523 roku we Francji. W wieku 23 lat rozpoczął karierę dyplomatyczną na dworze w Wormancji. Podróżował po całej Europie i rok później został przyjęty na służbę u księcia de Nevers. W roku 1549, podczas misji dyplomatycznej w Rzymie, Vigenere po raz pierwszy zetknął się z kryptografią. Ogromnie zafascynowany sztuką „tajnego pisma" oddał się studiowaniu książek największych kryptologów oraz własnym badaniom. Miał również możliwość współpracy z najwybitniejszymi ekspertami kurii papieskiej, co pozwoliło mu znacznie pogłębić wiedzę. Dzięki niej i bogatemu doświadczeniu został sekretarzem samego króla. W końcu, w wieku 47 lat postanowił opuścić dwór i zająć się pisaniem książek.

W roku 1586 Vigenere opublikował *Traktat o szyfrach*. Podobnie jak w dziele Trithemiusa, tak i tutaj znajdują się liczne dygresje na tematy zupełnie niezwiązane z kryptografią, za to jak najbardziej związane z czarną magią. Autor zachował mimo to naukową solidność w tych fragmentach książki, które w ogóle miały coś z nauką wspólnego. Opisał również własny szyfr polialfabetyczny.

System opracowany przez Vigenere'a polegał na szyfrowaniu kolejnych liter wiadomości za pomocą różnych wierszy tablicy Trithemiusa. Różnica polegała na sposobie wyboru kolejnego wiersza szyfrującego. Dla pierwszej litery mógł to być wiersz 17., dla drugiej — 5., dla trzeciej — 13. itd. W ten sposób znajomość samego systemu przestawała wystarczać do odszyfrowania wiadomości. Trzeba było jeszcze znać kombinację wierszy zastosowaną w danym przypadku. Nadawca i odbiorca mogli sobie ułatwić zapamiętanie tej kombinacji, ustalając specjalne słowo-klucz. Jego litery stanowiły jednocześnie pierwsze litery kolejno stosowanych wierszy szyfrowania. Dla przykładu, słowo kluczowe *sekret* oznaczało, iż do zaszyfrowania pierwszej litery wiadomości zastosowano 19. wiersz tabeli, dla drugiej — 5., dla trzeciej — 11. itd. Znajomość słowa-klucza wystarczała adresatowi do odszyfrowania wiadomości. Odszukiwał on kolejne litery szyfrogramu w odpowiadających im linijkach tabeli, po czym odczytywał literę tekstu jawnego z linijki znajdującej się na samej górze.

Vigenere stworzył również dwa systemy szyfrowania oparte na koncepcji autoklucza. W pierwszym przypadku kluczem stawał się odszyfrowywany tekst jawny. Konieczna była jedynie znajomość pojedynczej litery, stanowiącej tzw. ***klucz pierwotny***. Dzięki niej adresat odczytywał pierwszą literę tekstu jawnego, którą wykorzystywał do odczytania drugiej itd.

Drugi system z autokluczem również wykorzystywał klucz pierwotny. Tutaj jednak po zaszyfrowaniu pierwszej litery tekstu jawnego jej odpowiednik w kryptogramie stawał się kolejną literą klucza. Obie metody były znacznie bardziej innowacyjne i błyskotliwe niż opracowany przez Vigenere'a szyfr polialfabetyczny, jednak z niewiadomych przyczyn uległy zapomnieniu, a z nazwiskiem francuskiego uczonego kojarzony jest głównie szyfr oparty o tabelę Trithemiusa. Warto również zaznaczyć, iż koncepcja autoklucza została pierwotnie opisana przez włoskiego matematyka Girolamo Cardano, jednak opracowany przez niego system był pełen niedoskonałości i dopiero udoskonalenia wprowadzone przez Vigenere'a pozwalały na wykorzystanie tej metody przy szyfrowaniu wiadomości.

Szyfr Vigenere'a przez bardzo długi czas uchodził za niemożliwy do złamania. Zyskał nawet przydomek *le chiffre indechiffrable* (pol. szyfr nieodszyfrowywalny). Został złamany dopiero w XIX wieku przez brytyjskiego uczonego Charlesa Babbage'a.

1.3.2.4. Złamanie szyfru „nie do złamania"

Charles Babbage urodził się w roku 1792. Pochodził z bogatej rodziny (jego ojciec był bankierem), co pozwoliło mu na rozwijanie różnorodnych zainteresowań, w tym tych dotyczących kryptografii. Już jako dziecko zdradzał wyjątkowy talent w tej dziedzinie, przez co nieraz wpadał w kłopoty — łamał szyfry swoich szkolnych kolegów, a ci w rewanżu spuszczali mu lanie. Wraz z upływem lat rozwijał swoje umiejętności, aż stał się znany w całej Anglii. Często pomagał w przygotowywaniu materiału dowodowego w prowadzonych sprawach sądowych poprzez odszyfrowywanie korespondencji z nimi związanej. W roku 1854 zainteresował się problemem kryptoanalizy szyfru Vigenere'a. Nie przejmując się opiniami, jakoby szyfr ten był nie do złamania, rozpoczął poszukiwanie punktu zaczepienia, który pozwoliłby na skuteczną kryptoanalizę. Jeszcze w tym samym roku dokonał przełomowego odkrycia.

Babbage zauważył mianowicie, że jeśli pozna się długość użytego słowa-klucza, rozszyfrowanie tekstu będzie o wiele łatwiejsze, gdyż będzie wtedy wiadomo, które litery zaszyfrowane są przy użyciu takich samych podstawień. Na przykład jeśli słowo kluczowe ma 5 liter, to co piąta litera tekstu jest szyfrowana przy użyciu identycznego alfabetu. Wystarczy zatem podzielić tekst na grupy liter szyfrowane tą samą literą klucza i dokonać kryptoanalizy opartej na analizie częstości. Grupy te są bowiem niczym innym, jak prostym szyfrem podstawieniowym.

Oczywiście, kryptoanalityk nie zna długości klucza, informację tę można jednak zdobyć podczas badania kryptogramu. Przy dłuższych tekstach często zdarzają się bowiem powtórzenia wyrazów lub ich fragmentów szyfrowane tym samym fragmentem klucza. W takiej sytuacji w kryptogramie wystąpią powtarzające się kombinacje liter. Analizując odległości między nimi, ustalić można najbardziej prawdopodobną długość klucza. Z reguły jest nią jeden ze wspólnych dzielników tych odległości. Jeśli zatem udało nam się wyodrębnić cztery takie przypadki, a odstępy wynoszą 8, 16, 20 i 23 litery, to możemy z dużą dozą prawdopodobieństwa przyjąć, iż długość klucza wynosi cztery. Czasem powtórzenie może być dziełem przypadku, a nie synchronizacji klucza i tekstu, dlatego też ostatnią wartość (23) można zignorować. Zawsze jednak warto odszukać jak najwięcej powtórzeń, gdyż dzięki temu uzyskujemy większą ilość materiału do analizy, a co za tym idzie — większą pewność co do wyznaczonej długości klucza.

Technika zastosowana przez Babbage'a została rozwinięta i usystematyzowana przez pruskiego wojskowego, Friedricha W. Kasickiego. W swojej książce *Die Geheimschriften und die Dechiffrir-kunst* (Tajne pisma i sztuka deszyfracji) szczegółowo opisał on metodykę łamania polialfabetów, począwszy od wyznaczania okresu klucza, a na analizie wyodrębnionych szyfrów monoalfabetycznych skończywszy. Książka stała się znana dopiero po jego śmierci w roku 1881 roku, a opracowaną metodę ochrzczono mianem ***analizy Kasickiego***.

1.3.3. Szyfry digraficzne

Szyfr digraficzny opiera się na szyfrowaniu par znaków. Tekst jawny dzielony jest na pary znaków, a następnie przekształcany w kryptogram według ustalonego wzoru. Każdy symbol w kryptogramie jest więc zależny od dwóch liter tekstu jawnego, co utrudnia złamanie szyfru. Szyfry digraficzne zaliczyć można do szerszej grupy szyfrów wieloliterowych (operujących na grupach liter).

Pierwszy znany szyfr digraficzny pochodzi z dzieła *De Furtivis Literarum Notis* autorstwa Giovanniego Battisty Porty — włoskiego uczonego z XVI wieku. Zawierało ono opis znanych ówcześnie szyfrów, lingwistycznych aspektów kryptografii, technik kryptoanalitycznych oraz autorskie propozycje technik szyfrowania. Autor umieścił w nim również liczne cenne wskazówki dotyczące zarówno szyfrowania, jak i łamania szyfrów. To Porta jako pierwszy wpadł na pomysł kryptoanalizy opartej o prawdopodobieństwo występowania słów w tekście. Mówiąc najogólniej, kryptoanalityk znający przeznaczenie danej wiadomości może spróbować odszukać w tekście wyraz często występujący w tekstach o takim charakterze. Na przykład dla meldunku wojskowego mogą to być wyrazy *atak*, *wróg*, *dowódca* itp.

Co ciekawe, Porta nie podzielał powszechnej opinii, jakoby szyfry polialfabetyczne były nie do złamania. Przypuścił wiele ataków na znane wówczas polialfabety i był bardzo blisko sukcesu. W jednym przypadku udało mu się na podstawie występujących powtórzeń określić długość klucza, jednak nie zrobił z tej informacji żadnego użytku. W rezultacie szyfry polialfabetyczne uznawane były za bezpieczne przez kolejnych 300 lat.

Pierwszym w historii literowym szyfrem digraficznym był szyfr Playfaira, nazwany tak od nazwiska angielskiego uczonego epoki wiktoriańskiej. Nazwa ta przylgnęła do tego szyfru, mimo iż tak naprawdę jego autorem był inny uczony, Charles Wheatstone. Obaj panowie byli jednak do siebie łudząco podobni, przez co notorycznie ich ze sobą mylono.

Szyfr Playfaira opierał się na tablicy o wymiarach 5x5, w którą wpisywano kolejne litery alfabetu. Można też ją było wypełnić w oparciu o słowo-klucz. W takim przypadku wpisywano je w tablicę (ignorując powtarzające się litery), a pozostałe litery wstawiano w puste miejsca w porządku alfabetycznym. Rysunek 1.7 przedstawia tablicę utworzoną w oparciu o słowo *Playfair*.

Rysunek 1.7. *Tablica szyfru Playfaira*

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

Szyfrowanie rozpoczynano od podzielenia tekstu jawnego na pary znaków (*i* oraz *j* traktowano jako ten sam znak, natomiast pary takich samych liter należało oddzielić literą *x*). Następnie przekształcano wiadomość w kryptogram w oparciu o następujące zasady:

- Jeśli obie litery znajdowały się w tym samym rzędzie, były zastępowane literami znajdującymi się bezpośrednio po ich prawej stronie. Obowiązywała tutaj zasada cykliczności, tzn. ostatnia litera w rzędzie była zastępowana pierwszą po lewej.
- Jeśli obie litery znajdowały się w tej samej kolumnie, zastępowano je literami znajdującymi się pod spodem. Tutaj również obowiązywała zasada cykliczności.
- Litery znajdujące się w innych kolumnach i wierszach były zastępowane literami z tego samego wiersza, ale znajdującymi się w kolumnie drugiej litery tekstu jawnego.

Być może brzmi to nieco zawile. Łatwiej będzie zrozumieć to na przykładzie. Zaszyfrujemy wiadomość o treści: *tekst jawny* w oparciu o tablicę zamieszczoną na rysunku 1.7. Po podziale na pary znaków otrzymujemy: *TE KS TJ AW NY*. Litery T i E znajdują się w różnych kolumnach i wierszach, dokonujemy zatem podstawienia zgodnie z trzecią z wymienionych powyżej zasad — T zamienia się w N, a E w M. Kolejna para liter znajduje się w tej samej kolumnie, zastosowanie ma zatem zasada druga. W rezultacie otrzymujemy wynik SX. W przypadku trzeciej pary ponownie wykorzystujemy zasadę trzecią, przez co TJ zamienia się w ND. Czwarta para liter szyfrowana jest z użyciem zasady drugiej (AW przechodzi w BA), natomiast piąta — z użyciem zasady trzeciej (NY przechodzi w SP).

Szyfry digraficzne są trudniejsze do złamania za pomocą analizy częstości. Liczba digrafów jest zawsze o wiele większa niż liczba liter alfabetu jawnego (na przykład dla 26 liter mamy 676 digrafów) i mają one bardziej równomiernie rozłożoną częstość występowania.

1.3.4. Kamienie milowe kryptografii

Ogromny wpływ na rozwój kryptografii miało wynalezienie telegrafu. Umożliwiło ono komunikację na niespotykaną dotąd skalę i wywołało dyskusję na temat poufności przekazywanych informacji. W obawie przed nieuczciwymi telegrafistami wiele osób opracowywało własne szyfry „nie do złamania". Powstawały też liczne książki kodowe spełniające podwójne funkcje — oprócz ochrony tajnych informacji pozwalały one zmniejszyć koszt wysyłanych wiadomości. W książkach takich pojedyncze słowa kodowe odpowiadały bowiem całym zdaniom w tekście jawnym, przez co telegram stawał się krótszy.

Telegraf zmienił również oblicze wojny, która teraz mogła być prowadzona na znacznie większym obszarze. Dowódca mógł kontrolować wiele rozproszonych oddziałów i reagować znacznie szybciej na zachodzące na polu walki zmiany. Tutaj szyfrowanie

było jeszcze istotniejsze, gdyż przechwycenie meldunków przez wroga mogło kosztować życie wielu ludzi. Powstawały zatem liczne szyfry polowe, nieraz oparte na pomysłach kryptologów-amatorów. Wbrew pozorom opracowanie dobrego szyfru polowego nie było prostym zadaniem. Musiał on bowiem być nie tylko trudny do złamania, ale również prosty w implementacji. Podczas bitwy nie było czasu na przeprowadzanie wielu skomplikowanych obliczeń i przekształceń, a nieodłączny w takiej sytuacji stres mógł być przyczyną błędów w szyfrowaniu. Dobry szyfr polowy musiał zatem być prosty i skuteczny zarazem.

Kolejny rozkwit rozmaitych metod i technologii kryptograficznych przyniosła I wojna światowa. Oprócz telegrafu w powszechnym użyciu było już także radio, co zwiększało potencjał komunikacyjny, wymuszając jednocześnie większą dbałość o ochronę przekazywanych informacji. W tym ostatnim wypadku do podsłuchania przekazu nie trzeba już było uzyskiwać dostępu do linii telegraficznej — wystarczyło prowadzić nasłuch na odpowiedniej częstotliwości. Należało zatem liczyć się z faktem, iż każda wysłana w ten sposób informacja trafia w ręce wroga i może być odczytana, jeśli chroniący ją szyfr nie jest wystarczająco silny. Po obu stronach frontu pracowały więc całe sztaby ludzi prowadzących regularną kryptograficzną wojnę. Warto wspomnieć choćby brytyjski ***Pokój 40***, którego członkowie, łamiąc niemieckie szyfry, otworzyli swoim wojskom drogę do wielu spektakularnych zwycięstw, czy przytoczoną we wstępie historię złamania szyfru ADFGX.

Był to również okres wprowadzania licznych książek kodowych w komunikacji między oddziałami na froncie. Taki sposób zabezpieczania łączności miał jednak tę wadę, iż przechwycenie jednej z nich kompromitowało cały system. W związku z tym w razie groźby pojmania w pierwszej kolejności niszczono posiadane egzemplarze książek kodowych. Czasem jednak któraś z nich wpadała w ręce wroga, co powodowało konieczność opracowania i wysłania do wszystkich oddziałów nowych egzemplarzy. Tymczasem w przypadku dobrego systemu szyfrowania jedynym ryzykiem była utrata klucza.

Powstawały zatem kolejne szyfry i kody, a kryptografia stawała się coraz bardziej popularna, jednak z naukowego punktu widzenia nie dokonano wówczas żadnego istotnego przełomu. Prawdziwie rewolucyjne zmiany przynieść miała dopiero kolejna wojna.

1.4. Kryptografia II wojny światowej

Niewiele osób zdaje sobie sprawę, że to właśnie potrzeby kryptoanalityków okresu II wojny światowej doprowadziły do zaprojektowania i skonstruowania pierwszego komputera. Przyczyna była dość pragmatyczna — łamanie szyfrów stało się bardzo skomplikowane obliczeniowo i konieczne stało się odciążenie kryptoanalityków z wykonywania żmudnych przeliczeń. Istnienie takiej maszyny przez długie lata objęte było tajemnicą wojskową, a oficjalnie za pierwszy komputer jeszcze do niedawna uznawano ENIAC. Duży wpływ na jej powstanie miał wkład polskich naukowców, ale — jak mawia pewien znany historyk — nie uprzedzajmy faktów.

1.4.1. Enigma i Colossus

Wszystko zaczęło się od zastosowania przez niemiecką armię nowej wirnikowej maszyny szyfrującej — słynnej Enigmy (rysunek 1.8).

Rysunek 1.8.
Enigma



Wywiad aliantów znał schemat zarówno cywilnej, jak i wojskowej wersji niemieckiej maszyny jeszcze przed wojną, jednak naukowcy uznali, że zastosowany w niej algorytm szyfrujący uniemożliwia złamanie szyfru. Istotnie, był on wyjątkowo trudny do kryptoanalizy, jednak głównym powodem niewielkiego zainteresowania Enigmą był panujący krajach byłej koalicji po zakończeniu I wojny światowej brak poczucia zagrożenia ze strony Niemiec. Tymczasem Polska, która niedawno odzyskała niepodległość, obawiała się dalszego rozwoju stosunków z Niemcami, zwłaszcza po dojściu do władzy Adolfa Hitlera. Założono więc biuro szyfrów i podjęto kroki w celu poznania systemu szyfrowania zachodnich sąsiadów.

1.4.1.1. Jak działała Enigma?

Enigma była jedną z popularnych wówczas *maszyn wirnikowych*. Pierwszą taką maszynę skonstruował amerykański wynalazca Eduard Hugo Hebern. Jego wynalazek stanowiły dwie połączone elektryczne maszyny do pisania. Naciśnięcie klawisza w jednej

z nich powodowało uruchomienie czcionki w drugiej. Połączenia były zmodyfikowane, a więc wstukiwane litery ulegały zamianie na inne, w rezultacie dając prosty szyfr monoalfabetyczny. Kable przebiegały przez wirniki, które można było obracać, zmieniając tym samym schemat połączeń. W swojej pierwszej maszynie Hebern zamontował pięć walców, każdy o 26 możliwych ustawieniach. Można je było obracać względem siebie, co dawało łącznie 26^5 możliwych schematów połączeń. Odpowiada to szyfrowi Vigenere'a z kluczem o długości około 12 000 000 znaków.

Równolegle do Heberna podobną maszynę wynalazł holenderski uczony Hugo Aleksander Koch, a także niemiecki inżynier Artur Scherbius. Ten drugi zaproponował swój wynalazek armii niemieckiej już w 1918 roku, jednak wówczas nie spotkał się on z większym zainteresowaniem. Sytuacja zmieniła się po dojściu do władzy Hitlera. W ramach powszechnej modernizacji armii postanowiono wyposażyć niemieckie oddziały w maszyny szyfrujące. Wybór padł na maszynę Scherbiusa.

Enigma oprócz układu wirników wyposażona była w tzw. *walec odwracający*. Dzięki niemu możliwe było wykorzystanie maszyny zarówno do szyfrowania, jak i do deszyfrowania wiadomości. Co ciekawe, o ile z praktycznego punktu widzenia była to niewątpliwa zaleta, o tyle kryptograficznie stanowiło to poważną wadę. Taka konstrukcja powoduje bowiem powstanie ***negatywnego wzorca***, czyli, innymi słowy, zbioru zasad ograniczających liczbę możliwych kryptogramów. W tym przypadku żadna litera tekstu jawnego nie mogła zostać zaszyfrowana jako ona sama (czyli *A* w *A*, *B* w *B* itd.). Wiedza o tym okazała się bardzo cenna dla polskich, a później angielskich kryptoanalityków.

Wirniki Enigmy miały zdefiniowany układ połączeń, jednak można je było wkładać do urządzenia w różnej kolejności. Dodatkowo było ich więcej niż przeznaczonych na nie w maszynie gniazd (na początku wojny wirników było osiem). Każdy z nich można było ustawić na 26 sposobów. Podczas szyfrowania pierwszy z wirników obracał się o jedną pozycję z każdą szyfrowaną literą. Jego pełny obrót powodował przesunięcie o jedną pozycję drugiego wirnika, ten z kolei musiał wykonać pełny obrót, zanim o jedną pozycję przesunął się wirnik trzeci itd. Reasumując, o rodzaju zastosowanego przypisania decydowały następujące czynniki:

- wybór wirników szyfrujących,
- kolejność wirników w maszynie,
- początkowe pozycje wirników.

Na rysunku 1.8 widać Enigmę z czterema gniazdami wirników. Po naciśnięciu klawisza odpowiadającego literze tekstu jawnego na znajdującym się powyżej panelu podświetlana była litera tekstu tajnego. Szyfrowanie oparte było o system kluczy dziennych determinujących ustawienie wirników. Często już pierwsza litera wiadomości powodowała przesunięcie nie tylko pierwszego, ale również drugiego, a nawet trzeciego wirnika. Szyfrant zapisywał tekst tajny, po czym przekazywał go radiotelegrafiście. Dla uzyskania dodatkowego bezpieczeństwa korzystano również z osobnych kluczy dla poszczególnych depesz. Klucz taki był szyfrowany kluczem dziennym na początku wiadomości. Dla pewności powtarzano go dwa razy. Odbiorca deszyfrował klucz depeszy, po czym zmieniał zgodnie z nim ustawienia maszyny i odczytywał przekaz.

Wiedza na temat zasad stosowania kluczy dla poszczególnych wiadomości była kolejnym ułatwieniem dla polskich kryptoanalityków. Wiedzieli bowiem, iż na początku każdego kryptogramu znajduje się powtórzona dwukrotnie kombinacja liter, co pozwalało uzyskać cenne informacje na temat klucza dziennego oraz ustawienia wirników. Równie cenne okazało się lenistwo niemieckich szyfrantów, którzy wielokrotnie powtarzali ten sam klucz.

Nie bez znaczenia była również niemiecka pedantyczność i sformalizowany charakter nadawanych depesz. Komunikaty zaczynały się i kończyły w identyczny sposób, zawierały również liczne powtórzenia samej treści. Innymi słowy, niemieccy szyfranci byli bardzo przewidywalni. Dawało to dodatkowe informacje na temat zawartych w depeszy wyrazów i zwrotów.

1.4.1.2. Cyklometr i Bomby

W roku 1927 polskie służby celne przechwyciły jeden z egzemplarzy Enigmy wysłany do niemieckiej firmy w charakterze zaopatrzenia. Polacy zakupili później kolejne cywilne egzemplarze maszyny. Pomogły one w poznaniu zasad działania ich wojskowych odpowiedników. Rozpracowywaniem niemieckiego szyfru zajmowali się trzej naukowcy — Marian Rejewski, Henryk Zygalski i Jerzy Różycki. Dodatkową pomocą były dla nich dane udostępnione przez francuski wywiad. We Francji uznano Enigmę za niemożliwą do złamania, materiały te nie miały zatem dla francuskich naukowców większej wartości.

Niemcy ciągle doskonalili Enigmę (na przykład dodając kolejne wirniki), przez co łamanie szyfru stawało się coraz trudniejsze. Przede wszystkim rosła liczba koniecznych obliczeń. W końcu polscy matematycy postanowili zaprojektować specjalną maszynę, której zadanie polegałoby wyłącznie na wyszukiwaniu typowych permutacji występujących podczas szyfrowania za pomocą niemieckiej maszyny. Nie była to więc maszyna szyfrująca ani deszyfrująca, a jedynie narzędzie wspomagające obliczenia wykonywane podczas łamania szyfru. Urządzeniu nadano nazwę *Cyklometr*.

Szyfranci armii niemieckiej ustawicznie zwiększali złożoność algorytmu szyfrującego używanego w Enigmie i wkrótce Cyklometr nie był już w stanie wykonywać odpowiedniej liczby obliczeń. Dlatego skonstruowano nowe urządzenia obliczeniowe mające wspomagać kryptoanalizę szyfrów Enigmy. Urządzenia te nazwano *Bombami*.

Polski wywiad udostępnił Anglikom wyniki badań nad Enigmą w roku 1939. Jeszcze przed rozpoczęciem wojny polscy naukowcy (wraz z ich Bombami) zostali przewiezieni do Anglii. Tam badania były kontynuowane w słynnym Bletchley Park. Niestety, z niejasnych przyczyn polscy kryptoanalitycy nie zostali dopuszczeni do prac prowadzonych w tym miejscu. Powierzano im mniej istotne zadania, a z istnienia wielkiego ośrodka kryptoanalitycznego nawet nie zdawali sobie sprawy.

1.4.1.3. Bletchley Park

Centrum kryptoanalityczne w Bletchley Park powstało w wyniku poszerzenia personelu utworzonego w czasie I wojny światowej ***Pokoju 40***. Początkowo zatrudniano tam głównie filologów i lingwistów, jednak po spektakularnym sukcesie trzech polskich

matematyków postanowiono poszerzyć profil wykształcenia pracowników. Nowo zatrudnionych kierowano do Rządowej Szkoły Kodów i Szyfrów (GC&CS), a ta znajdowała się właśnie w ulokowanym w Buckinghamshire Bletchley Park. Znajdujący się tam niewielki pałacyk stał się brytyjskim centrum łamania szyfrów. W miarę przybywania nowego personelu w otaczających go ogrodach dobudowywano kolejne baraki i poszerzano specjalizację poszczególnych działów. Wkrótce podział ten w naturalny sposób wiązał się z przynależnością do określonego baraku. Dla przykładu barak 8 specjalizował się w kryptoanalizie depesz niemieckiej marynarki wojennej.

Po opanowaniu polskich metod kryptoanalitycznych specjaliści z Bletchley Park szybko zaczęli opracowywać własne techniki kryptoanalityczne. Jednym z najwybitniejszych pracowników centrum był Alan Turing. Opierając się na analizie archiwalnych kryptogramów, doszedł on do wniosku, iż często możliwe jest przewidzenie fragmentów depesz na podstawie ogólnych informacji na ich temat. Jeśli kryptoanalityk wie, iż w tekście musi się pojawić dany wyraz, może z dużym prawdopodobieństwem ustalić jego pozycję, korzystając z zasady negatywnego wzorca. Jak pamiętamy, żadna litera nie mogła zostać przekształcona w wyniku szyfrowania w nią samą, co eliminuje bardzo wiele potencjalnych pozycji wyrazu w tekście. Kryptoanalityk przesuwał pasek z wyrazem lub zwrotem pod treścią kryptogramu, analizując powstające w pionie pary liter. Pozycję można było odrzucić, jeśli dawała się wyróżnić chociaż jedna para identycznych liter. Spójrzmy na rysunek 1.9:

Rysunek 1.9. *Kryptoanaliza Enigmy oparta na negatywnym wzorcu*

Pozycja początkowa:

Kryptogram:	G	S	A	G	K	F	I	H	U	B	F	O	V	D
Badany wyraz:	A	N	G	R	I	F	F							

Pierwsze przesunięcie:

Kryptogram:	G	S	A	G	K	F	I	H	U	B	F	O	V	D
Badany wyraz:		A	N	G	R	I	F	F						

Drugie przesunięcie:

Kryptogram:	G	S	A	G	K	F	I	H	U	B	F	O	V	D
Badany wyraz:			A	N	G	R	I	F	F					

Trzecie przesunięcie:

Kryptogram:	G	S	A	G	K	F	I	H	U	B	F	O	V	D
Badany wyraz:				A	N	G	R	I	F	F				

Kryptoanalityk zakłada w tym przypadku, iż gdzieś w kryptogramie znajduje się słowo „angriff" (niem. atak). Przykłada zatem pasek z tym wyrazem pod kryptogramem. W pozycji początkowej pojawia się para liter F. Można ją zatem odrzucić gdyż, jak pamiętamy, żadna litera nie mogła zostać zaszyfrowana jako ona sama. Po pierwszym przesunięciu pojawia się z kolei para liter - G. Oznacza to, iż również na tej pozycji nie może się znajdować szukane słowo. Kolejne przesunięcie daje aż dwie pary takich

samych liter (A i I). Dopiero za czwartym razem udaje się znaleźć miejsce gdzie (teoretycznie) mógłby się znajdować poszukiwany wyraz. Kolejne dwa przesunięcia również nie dadzą pozytywnego wyniku ze względu na znajdującą się na pozycji jedenastej w kryptogramie literę F, jednak przesunięcie szóste ujawni następną możliwą pozycję wyrazu w kryptogramie (nie pojawią się żadne pary takich samych liter).

Turing udoskonalił również Bomby, przystosowując je do zmieniającej się struktury niemieckiego szyfru i wprowadzając własne poprawki dotyczące zarówno efektywności działania, jak i zastosowanych algorytmów. Na dobrą sprawę skonstruował on więc zupełnie nowe urządzenia, choć oparte na pomyśle polskiego kryptoanalityka. Maszyny wykorzystywano do poszukiwania ustawień wirników, które przekształcałyby podany wyraz w określony kryptogram. Ogólnie więc metodyka łamania Enigmy opierała się na wyszukiwaniu prawdopodobnych wyrazów w tekście, aby następnie ustalić wartości klucza na podstawie tak uzyskanej relacji „tekst jawny – kryptogram".

Dzięki przeprowadzonej przez Turinga analizie niemieckiego szyfru oraz udoskonalonym przez niego Bombom możliwe było dalsze odczytywanie niemieckich przekazów radiowych mimo rosnącej złożoności stosowanych szyfrów. Warto wspomnieć, iż tak naprawdę w niemieckiej armii funkcjonowało kilka różnych kryptosystemów — inny szyfr miała na przykład marynarka, a nieco inny — siły lądowe. Stosowane były inne wirniki i modele Enigmy, a i sami szyfranci cechowali się różnym stopniem profesjonalizmu. Tym niemniej z większym lub mniejszym trudem pracownicy Bletchley Park dzień w dzień odkrywali przed alianckim dowództwem zamiary i sekrety niemieckiej armii.

1.4.1.4. Colossus

W Bletchley Park nie zajmowano się jedynie Enigmą. Był to co prawda najpopularniejszy, ale nie jedyny szyfr niemiecki. Do wymiany wiadomości między najwyższymi rangą wojskowymi Trzeciej Rzeszy używano tzw. *przystawki szyfrującej*. Było to urządzenie opracowane w firmie Lorenz. Wykorzystywało ono kod opracowany przez francuskiego wynalazcę J.M.E. Baudota. W kodzie tym każdy znak reprezentowany był w systemie dwójkowym z wykorzystaniem taśmy perforowanej. Jedynce odpowiadała dziura w taśmie, a zeru — jej brak. Przystawka odczytywała jednocześnie dwie taśmy (jedna zawierała tekst jawny, a druga klucz), wykonując na odczytanych wartościach operację dodawania bez przenoszenia reszt (innymi słowy, dodawania modulo 2 — patrz rozdział 2.). Wynik zapisywany był na trzeciej taśmie.

Ten system szyfrowania był o wiele bardziej wyszukany niż stosowany w Enigmie, jednak i tutaj Anglicy odnieśli sukces. Po raz kolejny trzeba było wykorzystać maszyny do przeprowadzania niezbędnych obliczeń. W tym wypadku Bomby już nie wystarczały. Należało skonstruować nowe urządzenie, operujące na podobnej zasadzie jak niemiecka przystawka. Tak powstał Colossus.

Colossus opierał się na teoretycznym modelu opracowanym przez Alana Turinga. W odróżnieniu od Bomb, które były urządzeniami elektromechanicznymi, był urządzeniem elektronicznym. Zawierał półtora tysiąca lamp (dwa i pół tysiąca w późniejszych modelach) i potrafił zapamiętywać dane do dalszego przetwarzania. Czyniło to z niego pierwsze urządzenie, które można nazwać komputerem. Pierwszy model Colossusa

oddano do użytku w roku 1943, a więc trzy lata przed słynnym komputerem ENIAC. Ponieważ jednak jego istnienie owiane było tajemnicą wojskową, świat dowiedział się o nim dopiero w roku 1975, po odtajnieniu dotyczących projektu akt.

Wkład alianckich kryptoanalityków w przebieg II wojny światowej był ogromny. Niemcy nie wierzyli, iż można złamać szyfr Enigmy, a tymczasem każdego dnia już po kilku godzinach od zmiany klucza pracownicy Bletchley Park odczytywali pierwsze kryptogramy i przesyłali je do dowództwa. Możliwość poznania zamiarów wroga była ogromnym atutem, o niczym jednak nie przesądzała. Podobnie jak w całej historii tajemnego pisma z odczytanego szyfru należało jeszcze zrobić odpowiedni użytek. Wiedzy tak zdobytej nie można było też nadużywać, by nie wzbudzić u Niemców podejrzeń, że ich system został skompromitowany.

Przesadą byłoby twierdzić, iż to kryptoanalitycy wygrali wojnę z Trzecią Rzeszą. Niemniej jednak gdyby nie ludzie tacy, jak Rejewski czy Turing, z pewnością potrwałaby ona kilka lat dłużej. Hitler zdążyłby użyć pocisków V1 i V2, zginęłyby również kolejne setki tysięcy ludzi. Bardzo możliwe, iż II wojna światowa zakończyłaby się dopiero po zrzuceniu bomb atomowych na Niemcy.

1.5. Era komputerów

Zastosowanie komputerów zasadniczo zmieniło dotychczasowe sposoby szyfrowania. Po pierwsze proces szyfrowania przebiegał teraz szybciej i mógł się opierać na znacznie bardziej skomplikowanym algorytmie. Należy pamiętać, że mechaniczne maszyny szyfrujące ograniczały złożoność algorytmu poprzez samą swoją konstrukcję. W przypadku komputerów ograniczenie to znikało, ponieważ można było zasymulować dowolnie skomplikowane urządzenie. Innymi słowy, można teraz było szyfrować wiadomości przy użyciu „wirtualnych" szyfratorów, których fizyczna konstrukcja byłaby niemożliwa do wykonania.

Ostatnia, najważniejsza zmiana, jaka nastąpiła dzięki zastosowaniu komputerów, dotyczyła poziomu szyfrowania. Do tej pory odbywało się ono na poziomie liter. Oparte na elektronicznych przełącznikach maszyny operowały jedynie na liczbach dwójkowych. Spowodowało to przejście z szyfrowania liter i znaków na szyfrowanie ciągów zer i jedynek, które w systemie komputerowym służą do zapisu danych. Wcześniej należało ustalić reguły konwersji znanych nam znaków na system binarny. Stąd też w latach sześćdziesiątych opracowano kod ASCII.

Liczby w kodzie ASCII można z łatwością przedstawić w postaci binarnej, co umożliwia ich zapis w komputerze. Po zapisaniu wiadomości w postaci dwójkowej można przejść do szyfrowania, które zasadniczo nie różni się od procesu szyfrowania w erze przedkomputerowej. Nadal podstawową metodą jest przestawianie elementów zapisanej wiadomości według określonego klucza i algorytmu tak, by dla osoby postronnej nie miały one większego sensu — z tą różnicą, że tutaj podstawowym elementem, na którym dokonuje się operacji szyfrowania, jest pojedynczy bit, a nie znak, jak to miało miejsce wcześniej. Jak wiadomo, aby zapisać jeden znak, potrzeba jednego bajta, czyli ośmiu bitów.



ASCII (skrót od ang. *American Standard Code for Information Interchange*) jest zestawem kodów, standardowo z zakresu 0 – 127 (dziesiętnie), przyporządkowanych przez ANSI (Amerykański Instytut ds. Standardów) poszczególnym znakom alfanumerycznym (litery alfabetu angielskiego i cyfry), znakom pisarskim oraz sterującym (typu nowa linia). Na przykład litera „a" jest zakodowana przy użyciu liczby 97. Ponieważ ASCII jest standardem 7-bitowym, a większość komputerów operuje na wielkościach 8-bitowych (bajtach), pojawił się również rozszerzony kod ASCII. Dzięki niemu możliwe stało się wprowadzenie znaków narodowych do stosowanego na danym komputerze alfabetu. W związku z tym obecnie wykorzystywane w ramach kodu ASCII znaki mogą się różnić w zależności od komputera. Aby uniknąć tego typu zróżnicowania, opracowano standard UNICODE składający się z 65 536 znaków, dzięki czemu możliwe jest definiowanie znaków w wielu różnych językach.

1.5.1. DES

Kryptologia komputerowa najszybciej rozwijała się w Stanach Zjednoczonych. Powstało tam wiele systemów kryptograficznych, jednak ze względu na specyfikę amerykańskiego prawa wkrótce pojawiła się konieczność ustalenia powszechnie obowiązującego standardu szyfrowania. W 1973 roku z propozycją takiego uniwersalnego systemu o nazwie Demon wystąpił Horst Feistel, niemiecki emigrant, który przybył do USA w 1934 roku. Nazwa wywodziła się od słowa *Demonstration*, a jej skrócona forma spowodowana była ograniczoną długością nazw plików w używanym przez twórcę standardu systemie. Później Demon został „przechrzczony" na Lucyfera (ang. *Lucipher*), co stanowiło swoistą grę słów (angielskie słowo *cipher* oznacza szyfr). Lucyfer był szyfrem blokowym, a więc jako dane wejściowe przyjmował bloki danych o ustalonej długości, zaś na wyjściu podawał bloki kryptogramu o takiej samej długości. Innymi słowy, podstawową jednostką przetwarzania nie były tu pojedyncze bity czy bajty, a całe bloki danych (patrz podrozdział 3.2). Feistel utworzył kilka wersji tego szyfru; najbardziej znana opierała się na kluczu 128-bitowym, niezwykle odpornym na ataki metodą pełnego przeglądu (sprawdzania wszystkich kluczy po kolei — patrz podrozdział 3.1).

Aby Lucyfer został przyjęty jako standard, musiał najpierw zostać przedłożony Narodowej Agencji Bezpieczeństwa (NSA). Organizacja ta starała się cały czas kontrolować pojawiające się na rynku narzędzia kryptograficzne. Jej głównym celem było ograniczanie tych zabezpieczeń w taki sposób, aby mogły być złamane przez rządowych kryptoanalityków, gdyby zachodziło podejrzenie, że zabezpieczone nimi dane mogą stanowić zagrożenie dla bezpieczeństwa państwa. Podobnie było w przypadku kryptosystemu Feistela.

Przestrzeń kluczy systemu Feistela została przez NSA bardzo ograniczona. Każdy kolejny bit długości klucza powoduje podwojenie tej przestrzeni, a tym samym podwojenie bezpieczeństwa systemu, przynajmniej w odniesieniu do *ataku wyczerpującego* (patrz podrozdział 3.1). Wynika z tego, że skrócenie klucza o jeden bit implikuje 50-procentowy spadek bezpieczeństwa szyfru (w tym kontekście można sobie wyobrazić, jak drastyczny spadek bezpieczeństwa powoduje redukcja klucza ze 128 do 56 bitów). System ten nadal był wystarczająco bezpieczny dla sektora prywatnego, jednak ogra-

niczenie wprowadzone przez NSA spotkało się ze zdecydowanym sprzeciwem pozarządowych środowisk kryptograficznych, które zdawały sobie sprawę z możliwości złamania tego szyfru przez agencję.

Ostatecznie jednak pomimo licznych protestów 23 listopada 1976 roku 56-bitowa wersja szyfru Lucyfer Feistela została oficjalnie przyjęta jako standard szyfrowania danych DES (skrót od ang. *Data Encryption Standard*).

1.5.2. Narodziny kryptografii asymetrycznej

Jedną z osób, które dążyły do przełamania kryptograficznego monopolu NSA, był Whit Diffie. Diffiemu marzył się system kryptograficzny wolny od problemu dystrybucji klucza. Jego koncepcja opierała się na założeniu dotąd uważanym za technicznie niemożliwe do zrealizowania — klucz szyfrujący miał być powszechnie dostępny. Jedną z niepodważalnych zasad kryptografii była zasada tajności tego klucza i używania go zarówno do szyfrowania, jak i deszyfrowania wiadomości. Diffie zaprojektował natomiast system oparty na dwóch kluczach szyfrujących. Para takich kluczy miała być tworzona dla każdego użytkownika jego systemu. Jeden z nich (klucz publiczny) miał służyć do szyfrowania wiadomości wysyłanych do użytkownika i miał być powszechnie dostępny. Drugi (klucz tajny) miał być wykorzystywany do dekryptażu wiadomości zaszyfrowanych przy użyciu pierwszego klucza. Za pomocą drugiego klucza można było również szyfrować wiadomości. W takim przypadku dekryptaż miał umożliwiać klucz publiczny. Dzięki takiej kombinacji możliwe stawało się uwierzytelnianie nadawcy wiadomości elektronicznej, ponieważ tylko osoba posiadająca klucz tajny mogła zaszyfrować dokument tak, aby dało się go odczytać przy użyciu klucza publicznego. Zaszyfrowanie wiadomości kluczem prywatnym stanowiło więc jednocześnie formę elektronicznego podpisu.

Sama teoria kluczy nie wystarczała i konieczne stało się opracowanie odpowiednich podstaw matematycznych, możliwych do zaimplementowania w językach programowania. Problem ten rozwiązał współpracownik Whita Diffiego — Marty Hellman. Hellman i Diffie wspólnie opracowali system matematyczny oparty na funkcji jednokierunkowej bazującej na tzw. logarytmowaniu dyskretnym (patrz rozdział 2.). System ten znany jest obecnie jako algorytm Diffiego-Hellmana.

System Diffiego i Hellmana nie tylko rozwiązał problem dystrybucji klucza, ale również zapoczątkował technologię elektronicznego uwierzytelniania użytkowników. Jego metoda rodzi bowiem jeszcze jedną istotną implikację, którą jest niemożliwość wyparcia się swojego cyfrowego podpisu. Skoro wiadomo, że technicznie niemożliwe jest, aby osoba nieznająca tajnego klucza wygenerowała poprawny podpis, jego właściciel nie może się wyprzeć swojego udziału w poświadczonej nim transakcji. Ta właściwość stała się podstawą technologii podpisu elektronicznego.

1.5.3. RSA

Idea kryptosystemu z kluczem publicznym została rozwinięta przez trzech naukowców z uniwersytetu w Stanford — Rona Rivesta, Adi Shamira i Leonarda Adlemana.

Podobnie jak Diffie i Hellman poświęcili oni dużo czasu na znalezienie matematycznego wzoru, który pozwalałby zrealizować ideę szyfrowania przy użyciu pary kluczy w praktyce. Przełomowego odkrycia podczas tych badań dokonał Rivest. Polegało ono na zastąpieniu algorytmu Diffiego-Hellmana jego własnym systemem obliczeń.

Koncepcja Rivesta opiera się na problemie rozkładu dużych liczb na czynniki pierwsze. Klucz publiczny generowany jest przez pomnożenie przez siebie dwóch dużych, losowo wybranych liczb pierwszych. Następnie wybierana jest kolejna duża liczba o określonych właściwościach — stanowi ona klucz szyfrujący. Klucz publiczny tworzony jest na podstawie klucza szyfrowania oraz wspomnianego iloczynu liczb pierwszych. Klucz prywatny można łatwo obliczyć, jeśli zna się liczby pierwsze tworzące iloczyn zastosowany przy tworzeniu klucza publicznego. Są one znane właścicielowi pary kluczy, natomiast kryptoanalityk może je uzyskać jedynie dzięki rozwiązaniu problemu faktoryzacji dużych liczb. Matematyczne szczegóły tej metody opisane zostały w rozdziale 2.

Algorytm opracowany przez Rivesta i jego współpracowników został wkrótce opatentowany pod nazwą RSA (od pierwszych liter nazwisk wynalazców). Agencja Bezpieczeństwa Narodowego próbowała zapobiec upowszechnieniu się tego standardu szyfrowania. Zaczęto wywierać naciski na NIST (skrót od ang. *National Institute of Standards and Technology*), aby przyjął jako obowiązujący w USA standard program DSA (skrót od ang. *Digital Signature Algorithm* — patrz dodatek B).

W wielu miejscach DSA powielał rozwiązania z RSA, jednak był systemem znacznie słabszym: „Pod względem czysto technicznym było jasne, że DSA był gorszy od RSA. Algorytm ten był, jak to wyłożył jeden z obserwatorów, »dziwacznym standardem«, o wiele wolniejszym od systemu RSA, jeśli chodzi o weryfikowanie podpisów (chociaż szybszym w podpisywaniu wiadomości), trudniejszym do wdrożenia i bardziej skomplikowanym. I nie umożliwiał szyfrowania. System opracowany przez rząd oferował jednak pewną korzyść w porównaniu z RSA […]. Był bezpłatny”[4].

Brak możliwości szyfrowania był poważną wadą techniczną systemu DSA, jednak poprzez rozprowadzanie go w charakterze darmowego oprogramowania NSA ustanowiła silną konkurencję dla standardu RSA (tym bardziej, że DSA stał się ustawowo ustalonym standardem).

1.5.4. PGP

Działalność NSA zmierzająca do ograniczenia dostępu do kryptografii powodowała konflikt między rządem a kryptoanalitykami sektora publicznego. Ci drudzy szukali sposobu na wprowadzenie kryptografii do powszechnego użytku. Zdawali sobie sprawę, że upowszechnienie komputerów, a zwłaszcza internetu, znacznie ograniczy prywatność zwykłych użytkowników, jeśli nie zagwarantuje się im odpowiednich zabezpieczeń. Z tego powodu Phil Zimmerman, programista z Florydy, rozpoczął projektowanie własnego systemu kryptograficznego. Nadał mu nazwę PGP (skrót od ang. *Pretty*

[4] Levy S., *Rewolucja w kryptografii*, Wydawnictwa Naukowo-Techniczne, Warszawa 2002.

Good Privacy — całkiem niezła prywatność). Początkowo miał to być kolejny komercyjny pakiet szyfrujący. Zamiary Zimmermana zmienił projekt opracowanej w Komisji Prawnej Senatu ustawy nr 266 z 24 stycznia 1991 roku. Zgodnie z nią dostawcy usług komunikacji elektronicznej, a także wytwórcy sprzętu komunikacyjnego powinni zapewnić rządowi możliwość uzyskania jawnej treści komunikacji między użytkownikami, jeśli uzyska on do tego upoważnienie prawne.

Zimmerman zdał sobie sprawę, że po wejściu ustawy w życie nie będzie już mógł wprowadzić na rynek swojego programu. Postanowił więc udostępnić go jak największej liczbie osób, zanim posługiwanie się nim przestanie być prawnie dozwolone. W tym celu postanowił wykorzystać internet. Skontaktował się ze swoim przyjacielem, Kellym Goenem, powierzając mu zadanie umieszczenia PGP 1.0 na powszechnie dostępnych sieciowych witrynach znajdujących się w USA. Wyznaczonego dnia Goen przy użyciu telefonów publicznych, laptopa i telefonu komórkowego wprowadził PGP do internetowych serwerów plików. Mógł go stamtąd ściągnąć każdy, kto miał dostęp do internetu, nie tylko w USA.

Phil Zimmerman zagwarantował prywatność każdemu, kto miał dostęp do jego programu. Ustawa 266 ostatecznie nie została wprowadzona w życie ze względu na protesty środowisk walczących o swobody obywatelskie. Była ona także niemożliwa do wyegzekwowania ze względu na powszechną dostępność pakietu PGP. Sam Zimmerman natomiast został pozwany do sądu przez RSA Data Security z powodu naruszenia praw patentowych algorytmu RSA (Zimmerman użył go w swoim programie, nie wiedząc, że RSA jest objęty ochroną patentową). Firma domagała się od niego wycofania PGP. Ostatecznie doszło do ugody, w myśl której autor PGP 1.0 zaprzestał dalszej dystrybucji swojego programu, a firma nie wniosła oskarżenia.

W 1993 roku Zimmerman został oskarżony o złamanie prawa przez rząd USA. Zdaniem FBI, udostępniając publicznie silny system kryptograficzny, Zimmerman dostarczył wrogim państwom oraz terrorystom narzędzie do walki z USA. Dochodzenie umorzono po trzech latach. Zresztą wydanie wyroku skazującego i tak nic by już nie zmieniło. Wycofanie PGP z powszechnego obiegu było niemożliwe, tak jak niemożliwe jest pełne kontrolowanie przepływu informacji w internecie.

Prawne restrykcje wobec twórców kryptograficznego oprogramowania były dość częstym środkiem stosowanym przez rząd USA w celu ograniczenia dostępu do kryptografii. Eksport oprogramowania z zakresu tzw. silnej kryptografii (opartej na większej niż ustalona długości klucza) był prawnie zakazany i traktowany na równi z nielegalnym eksportem broni. Sytuacja ta zmieniła się dopiero na początku obecnego stulecia, kiedy okazało się, że z uwagi na gwałtowny rozwój internetu niemożliwa jest dalsza kontrola nad rozprzestrzenianiem się oprogramowania, a tego typu ograniczenia osłabiają tylko gospodarkę USA. Firmy amerykańskie traciły zagranicznych klientów, gdyż nie były w stanie zagwarantować im takiego samego bezpieczeństwa danych, jak firmy spoza USA, nieobjęte ograniczeniami co do długości klucza.

Należy zauważyć, że posunięcie Zimmermana oprócz niewątpliwych korzyści dla zwykłych użytkowników sieci komputerowych mogło również spowodować znaczne szkody. Teraz bowiem każdy mógł zaszyfrować swoje komunikaty w ten sposób, że nikt

nie byłby w stanie ich odczytać. Innymi słowy, PGP umożliwia szyfrowanie korespondencji również terrorystom, miłośnikom dziecięcej pornografii i każdemu, kto wykorzystuje komputer do działalności przestępczej. Zimmerman zdawał sobie z tego sprawę, uznał jednak, że upowszechnienie pakietu będzie „mniejszym złem".

Wkrótce po udostępnieniu PGP program został poddany szczegółowej analizie przez grono specjalistów od kryptografii. Okazało się, że posiada on pewne wady ograniczające jego bezpieczeństwo. Postanowiono więc stworzyć nową wersję programu — PGP 2.0. Zastosowane w niej rozwiązania były stosowane także w późniejszych wersjach (aż do najnowszej — PGP 9). Dokładny opis PGP znaleźć można w rozdziale 4.

1.5.5. Ujawniona tajemnica

Warty wspomnienia jest fakt, że technika szyfrowania asymetrycznego została opracowana już w 1969 roku przez Jamesa Ellisa, pracownika angielskiego GCHQ (skrót od ang. *Government Communication Headquaters* — głównej rządowej kwatery łączności), jednak nie mógł on jej upowszechnić ze względu na obowiązującą go tajemnicę państwową. Efekty jego pracy zostały ujawnione dopiero niedawno, dlatego też informacje o nich można znaleźć jedynie w najnowszych opracowaniach z dziedziny kryptografii.

Pomysł Ellisa był bardzo podobny do systemu Whita Diffiego. Również opierał się on na idei pary kluczy szyfrujących. Podobnie jak Diffie, Ellis stworzył teoretyczne fundamenty systemu szyfrowania asymetrycznego i także nie był w stanie samodzielnie opracować wzoru matematycznego, na podstawie którego taki system mógłby funkcjonować. Przez kilka następnych lat wielu matematyków GCHQ zmagało się z tym problemem, jednak żaden nie znalazł rozwiązania. Sytuacja zmieniła się, kiedy zadanie to powierzono nowo zatrudnionemu matematykowi, Cliffordowi Cocksowi.

Klucz publiczny opracowany przez Cocksa opierał się, podobnie jak w systemie RSA, na iloczynie dwóch dużych liczb pierwszych. Iloczyn ten miał być dostępny dla każdego, kto chciał wysłać zaszyfrowaną wiadomość do odbiorcy. Cocks opracował następnie formułę matematyczną, dzięki której wiadomość zaszyfrowana przy użyciu klucza publicznego mogła być odszyfrowana jedynie pod warunkiem znajomości oryginalnych liczb pierwszych. Formuła zastosowana przez angielskiego matematyka była niemal identyczna z tą, którą zastosował Ron Rivest. Innymi słowy, Ellis i Cocks opracowali system, który trzy lata później został ponownie odkryty przez trzech matematyków z MIT i wprowadzony do powszechnego użytku jako RSA.

1.5.6. Upowszechnienie kryptografii

Spopularyzowanie kryptografii asymetrycznej doprowadziło do przełamania kryptologicznego monopolu NSA. Kryptografia cieszyła się coraz większym zainteresowaniem w sektorze publicznym, co utrudniało wszelkie próby ograniczania dostępu do opartych na niej zabezpieczeń. Mimo to agencja nadal starała się kontrolować rozwój badań nad nowymi technologiami z tego zakresu. Naukowcy, którzy nie pracowali dla

NSA, zobowiązani byli przedstawiać swoje artykuły przed ich publikacją specjalnie w tym celu utworzonej komisji. Jej zadaniem było wyławianie treści potencjalnie niebezpiecznych dla bezpieczeństwa narodowego. Na tym etapie była to już jednak walka skazana na niepowodzenie.

Na początku lat osiemdziesiątych zainaugurowano serię konwentów o nazwie Crypto, które odtąd odbywały się corocznie. Spotykali się na nich kryptolodzy z całego świata w celu wymiany doświadczeń i wyznaczania nowych kierunków badań. O ile jednak w tym przypadku NSA mogła się jeszcze pokusić o próby wpływania na prezentowane treści, o tyle prężnie rozwijający się internet stanowił medium, którego nawet agencja nie mogła sobie podporządkować. Raz zamieszczony w sieci artykuł lub program był ściągany i kopiowany przez niezliczone rzesze użytkowników, co uniemożliwiało jego wycofanie, nawet gdyby udało się przekonać do tego samego autora. Najlepszym przykładem jest tu PGP. Solą w oku NSA była w tamtym czasie grupa ludzi określających się jako *Szyfropunki*. Pisali oni programy, artykuły i opracowania z dziedziny kryptografii, a następnie udostępniali je w sieci. Oczywiście, nikt tu nie pytał NSA o zgodę. Grupka ta doskonale odzwierciedlała nastroje panujące w amerykańskim społeczeństwie, coraz bardziej wzburzonym rządowymi próbami kontrolowania przepływu informacji i ingerowania w prywatność obywateli. Wkrótce więc kryptograficzni anarchiści stali się ulubieńcami mediów i symbolem walki o swobody obywatelskie.

Kolejnym etapem kryptograficznych zmagań było zapoczątkowanie przez NSA w 1993 roku projektu ***EES*** (skrót od ang. *Escrowed Encryption Standard*) opartego na chipach *Capstone* i *Clipper*. Miały to być powszechnie dostępne urządzenia umożliwiające szyfrowany przekaz danych. Capstone służyć miał posiadaczom komputerów przenośnych, natomiast Clipper był przeznaczony do montowania w telefonach i faksach. Każde z urządzeń miało na trwałe zaimplementowany klucz szyfrowania, do którego służby rządowe mogły uzyskać dostęp, gdyby zachodziło podejrzenie, iż właściciel chipu prowadzi działalność niezgodną z prawem. Tak przynajmniej wyglądało to w teorii, nie da się jednak ukryć, że deponowanie kluczy dawało organizacjom rządowym ogromne pole do nadużyć. W rezultacie nie trzeba było długo czekać na protesty środowisk liberalnych. Były one tym bardziej uzasadnione, iż zastosowany w obu chipach algorytm Skipjack opracowany został w NSA i dane na jego temat były tajne. W rezultacie agencja miała monopol na produkcję obu urządzeń, a to budziło uzasadnione poniekąd podejrzenia co do prawdziwych intencji rządu. Ostatecznie NSA zdecydowała się upublicznić algorytm, jednak to jedynie pogorszyło sprawę. Jego kryptoanaliza przeprowadzona w środowiskach prywatnych wykazała bowiem, iż po pierwsze, nie jest on tak mocny jak AES, a po drugie, możliwe jest wykorzystanie go bez deponowania kluczy. Znacznie osłabiło to rozwój nowej technologii i ostatecznie udaremniło jej upowszechnienie na większą skalę.

Obecnie każdy może bez przeszkód korzystać z dobrodziejstw kryptografii. Nie jest ona domeną tylko i wyłącznie organizacji rządowych, choć z całą pewnością dysponują one pod tym względem znacznie większym potencjałem z uwagi na to, że skupiają najlepszych fachowców i inwestują w badania nad nowymi technologiami. Trudno powiedzieć, jakie dokładnie są możliwości agencji takich jak NSA w odniesieniu do kryptografii, z pewnością jednak możliwości „zwykłego śmiertelnika" zwiększyły się w ciągu ostatniego półwiecza niepomiernie.