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

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

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 (tabela 1.)

Tabela 1: 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.
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.

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" [2]

1.3 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 przed komputerowej. 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.

1.4 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. 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).

1.5 RSA

Idea kryptosystemu z kluczem publicznym została rozwinięta przez trzech naukowców z uniwersytetu w Stanford — Rona Rivesta, Adi Shamira i Leonarda Adlemana. 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. 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*).
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" [3]

Literatura

[1] Kahn D., *Łamacze kodów - historia kryptologi*, Wydawnictwo Naukowo-Techniczne, Warszawa 2004.

[2] Singh S., *The TEXbook*. Addison-Wesley, Reading, Massachusetts, 1983.

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