Historia i podstawy kryptografii
Spotkanie 8
Dalsze dzieje szyfrów polialfabetycznych

Jacek Rogowski

I Liceum Ogólnokształcące
w Łowiczu

Kryptoanaliza szyfru Vigenere'a

Złamanie szyfru Vigenere'a jest łatwe w dwóch przypadkach:

(1) jeżeli znany jest fragment tekstu jawnego, nawet wtedy, gdy nie jest znane miejsce występowania tego fragmentu,

(2) jeżeli znana jest długość klucza.

W pierwszym przypadku należy testować kolejne hipotezy:

> *zaszyfrowany znany tekst jest fragmentem kryptogramu zaczynającym się od jego n-tej litery,* $n = 1, 2, 3, 4, \ldots$.

Dla każdej takiej hipotezy posługując się tekstem tajnym i jawnym wyznaczany jest (fragment) hipotetycznego klucza, za pomocą którego odszyfrowuje się dalsze partie tekstu.
W przypadku trafienia na prawidłowe ustawienie tekstu jawnego znaleziony klucz pozwala na odczytanie dalszych sensownych fragmentów tekstu jawnego, które można uzupełnić (odgadnąć) i wykorzystać te uzupełnienia do dalszej kryptoanalizy.

Kryptoanaliza szyfru Vigenere'a

W drugim przypadku, gdy znana jest długość klucza n wszystkie litery tekstu jawnego odległe o $n-1$ miejsc są szyfrowane tym samym szyfrem Cezara (z nieznanym kluczem).
Analizując częstotliwości pojawiania się poszczególnych liter w tekście tajnym na miejscach k, $k+n$, $k+2n$, $k+3n$ itd. można ustalić klucz szyfru Cezara użytego do otrzymania tych liter, a więc można znaleźć k-tą literę klucza.

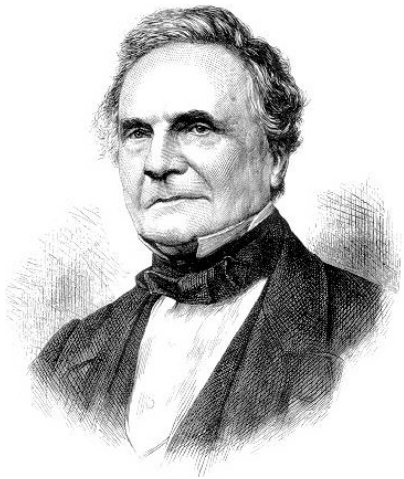
Problem

Jak wyznaczyć długość klucza szyfru Vigenere'a (bez znajomości fragmentu tekstu jawnego)?

Problem ten został rozwiązany w XIX w.

Kryptoanaliza szyfru Vigenere'a

W 1863 pruski oficer Friedrich Wilhelm Kasiski (1805 – 1881) opublikował książkę *Die Geheimschriften und die Dechiffrir-Kunst*, w której podał metodę znajdowania długości klucza szyfru Vigenere'a.



Wcześniej metodę tę odkrył angielski matematyk i mechanik Charles Babbage (1791 – 1871), ale jego odkrycie zostało utajnione przez władze wojskowe Wielkiej Brytanii.

Kryptoanaliza szyfru Vigenere'a

Kasiski powiązał ze sobą następujące fakty:

- pewne zbitki kilku liter (np. słowa lub ich części) występują w danym języku częściej niż inne,
- jeżeli takie zbitki liter występują w tekście jawnym w odległości będącej wielokrotnością długości klucza, to zostaną zaszyfrowane w ten sam sposób i w tekście tajnym będą reprezentowane przez takie same ciągi znaków,
- przypadkowe wystąpienie w szyfrogramie takich samych ciągów znaków, które nie odpowiadają tym samym zbitkom liter w tekście jawnym, jest możliwe, ale mało prawdopodobne.

Konsekwencją powyższych obserwacji jest procedura zwana **testem Kasiskiego**.

Kryptoanaliza szyfru Vigenere'a

Test Kasiskiego

- W tekście tajnym należy wyszukać wszystkie pary takich samych bloków liter złożonych z co najmniej dwóch liter, ale bardziej wiarygodne wyniki dają bloki trójliterowe lub dłuższe.
- Dla każdej takiej pary należy obliczyć, ile liter leży pomiędzy pierwszymi literami tych bloków i do każdego wyniku trzeba dodać 1.
- Dla otrzymanych liczb należy znaleźć ich najmniejszy wspólny dzielnik M większy od 1.
- Długość klucza jest wielokrotnością wyznaczonej liczby M.
- Trzeba pamiętać o możliwości błędnego wyznaczenia długości klucza, jeżeli przypadkowo różne ciągi liter w tekście jawnym zostały zaszyfrowane przez te same ciągi znaków.

Kryptoanaliza szyfru Vigenere'a

Przykład:

Przypomnijmy, że szyfrując tekst jawny

abrakadabra

z kluczem

projekt

otrzymaliśmy szyfrogram

PSFJOKWPSFJ.

Zbitką liter powtarzającą się w tekście tajnym jest PSFJ.
Liczba liter występujących pomiędzy dwoma powtórzeniami litery P wynosi 6.
Ponieważ $6+1=7$ jest liczbą pierwszą, to przyjmujemy, że $M=7$.
Klucz szyfru ma rzeczywiście długość 7.

Szyfr doskonały

W 1917 r. Gilbert Vernam (1890 - 1960) rozwinął ideę szyfru Vigenere'a i szyfru z autokluczem tworząc szyfr doskonały, który opiera się jakimkolwiek próbom jego złamania.

Algorytm szyfru Vernama

- Kluczem jest **losowy** ciąg liter o długości równej co najmniej długości szyfrowanego tekstu.
- Szyfrowanie odbywa się za pomocą tablicy Trithemiusa przy wykorzystaniu losowego klucza.
- Użyty klucz jest **kluczem jednorazowym**, tzn. może zostać użyty tylko w czasie jednej sesji szyfrowania/odszyfrowywania.

W praktyce szyfrowany tekst jest zapisywany w postaci ciągu binarnego, a klucz losowy jest zastępowany **pseudolosowym** ciagiem bitów.

Szyfr XOR

Operator logiczny $\oplus$

Operator logiczny $\oplus$ zwany *alternatywą wykluczającą* lub *XOR* działa na bitach i jest zdefinowany następująco:

$$0 \oplus 0 = 1 \oplus 1 = 0, \qquad 1 \oplus 0 = 0 \oplus 1 = 1.$$

Algorytm szyfru XOR

- Litery tekstu jawnego zapisywane są za pomocą ciągów binarnych ustalonej długości, np. w postaci kodu ASCII.
- Generowany jest pseudolosowy ciąg binarny (jednorazowy klucz).
- Szyfrowanie polega na wykonaniu operacji $\oplus$ na parach bitów złożonych z kolejnych bitów tekstu jawnego i bitów klucza.

Szyfr XOR — przykład

Tekst jawny: 100101

Klucz: **010110**

Szyfrowanie:

tekst jawny:	1	0	0	1	0	1
klucz:	**0**	**1**	**0**	**1**	**1**	**0**
tekst tajny:	1	1	0	0	1	1