Historia i podstawy kryptografii
Spotkanie 1
Pierwsze kroki

Jacek Rogowski

I Liceum Ogólnokształcące
w Łowiczu

Kiedy ludzie zaczęli szyfrować?

Odpowiedź:

Szyfry pojawiły się wraz z umiejętnością pisania i koniecznością przesyłania wiadomości bez ujawniania ich zawartości osobom nieupoważnionym.

Najstarsze szyfrowane zapiski pojawiły się

- w starożytnej Mezopotamii (pismo klinowe),
- w starożytnym Egipcie (pismo hieroglificzne),
- w starożytnym Izraelu (biblijny szyfr *atbasz*),
- w starożytnej Grecji (wzmianki w *Iliadzie*).

Co to jest kryptologia?

Odpowiedź tak ogólna, że aż niejasna:

Kryptologia jest nauką o wszystkich aspektach tajnego zapisywania wiadomości.

Co to jest kryptologia?

Elementy kryptologii

- *kryptografia*, czyli nauka o szyfrowaniu wiadomości, tzn. o metodach ukrywania ich znaczenia;
- *kryptoanaliza*, czyli nauka o odczytywaniu zaszyfrowanego tekstu bez uprzedniej znajomości klucza;
- *steganografia*, czyli nauka o ukrywaniu (istnienia) wiadomości.

Co to jest kryptologia?

Definicja szyfru

Szyfrem (lub *systemem kryptograficznym*) nazywamy system ukrywania znaczenia wiadomości przez zastąpienie każdego znaku oryginalnej wiadomości w ustalony sposób przez inny znak, przy czym zastąpienie to powinno być możliwe do jednoznacznego odwrócenia (odszyfrowania) przynajmniej dla adresata wiadomości.

Przykład: Podstawianie liter

Pomysłem najczęściej wykorzystywanym przy tworzeniu szyfrów jest zastąpienie każdej litery wiadomości (czyli: tekstu jawnego) przez inną literę przyporządkowaną jednoznacznie w ustalony sposób. Przyporządkowanie to nazywamy *kluczem* szyfru.

Zapamiętanie albo odtworzenie klucza można ułatwić następująco:

- wybieramy tajne słowo, które jest znane tylko nadawcy i odbiorcy wiadomości,
- wypisujemy kolejno litery alfabetu, którym się posługujemy,
- pod początkowymi literami alfabetu wpisujemy kolejne litery wybranego tajnego słowa; należy pominąć powtarzające się w nim litery,
- pod następnymi literami alfabetu wpisujemy kolejno te litery alfabetu, które nie wystąpiły w wybranym słowie,
- otrzymana tabela podstawień jest kluczem.

Przykład: Podstawianie liter

Tajne słowo: SZYFROWANIE.

Klucz:

a	b	c	d	e	f	g	h	i	j	k	l
S	Z	Y	F	R	O	W	A	N	I	E	B
m	n	o	p	r	s	t	u	w	y	z	
C	D	G	H	J	K	L	M	P	T	U	

Słowo *kryptografia* szyfrujemy następująco:

k	r	y	p	t	o	g	r	a	f	i	a
E	J	T	H	L	G	W	J	S	O	N	A

Przykład: szyfr „parkan”

Inny pomysł polega nie na *podstawianiu* (zastępowaniu liter innymi znakami), a na *przestawianiu* liter w ustalony sposób.
Przykładowym szyfrem tego typu jest tzw. szyfr „parkan”.

- Kolejne litery wiadomości wypisujemy pionowo w kolumnach o ustalonej długości; kluczem jest długość kolumny.
- Ostatnią kolumnę w razie potrzeby uzupełniamy dowolnie wybranymi literami.
- Tekstem zaszyfrowanym są wiersze otrzymanej tablicy.

Przykład: szyfr „parkan”

Klucz: Liczba 4

Tekst jawny:

kryptografia jest pełna niespodzianek

Szyfrowanie:

k	t	a	j	p	a	s	z	e
r	o	f	e	e	n	p	i	k
y	g	i	s	ł	i	o	a	a
p	r	a	t	n	e	d	n	b

Tekst tajny:

KTAJP ASZER OFEEN PIKYG ISŁIO AAPRA TNEDN B.

Przykład: steganografia

Przyjrzyjmy się niewinnie wyglądającej wiadomości:

W spa jest bardzo przyjemnie, ale
drogo. Wcale jednak nie tęsknię do
domu. Właściwie zamierzam jeszcze
prosto stąd pojechać do Krakowa na
początku tygodnia, lecz nie wiem,
czy mi się to uda.

A teraz zwróćmy uwagę na trzecią literę od lewej w każdym wierszu. Czytając te litery z góry w dół otrzymujemy wiadomość:

POMOCY.