Historia i podstawy kryptografii
Spotkanie 3
Dwa ważne szyfry starożytności

Jacek Rogowski

I Liceum Ogólnokształcące
w Łowiczu

Umowa notacyjna

Tekst (i alfabet) jawny będzie zapisywany przy użyciu małych liter, a tekst (i alfabet) tajny — za pomocą DUŻYCH.

Szyfr Cezara

Gajusz Juliusz Cezar używał wielu szyfrów w czasie swoich licznych kampanii wojskowych. Informacje o jednym z nich przekazał żyjący około 130 lat później rzymski historyk Swetoniusz. Zgodnie z jego relacją Cezar stosował następujący

Algorytm szyfrowania:

- Załóżmy, że używany alfabet ma n liter.
- Ustalmy liczbę całkowitą k, która spełnia nierówność $1 \leqslant k < n$. Liczba k jest kluczem szyfru.
- Każdą literę wiadomości jawnej zastępujemy literą leżącą w alfabecie o k miejsc dalej, przy czym k ostatnich liter w alfabecie zastępuje się kolejno literami A, B, C, ... (lub A, Ą, B, ... w przypadku używania pełnego polskiego alfabetu).

Uwaga

Szyfr Cezara jest szyfrem podstawieniowym monoalfabetycznym.

Szyfr Cezara — przykład

Klucz: $k = 3$.

Alfabet: polski uproszczony.

Tabela podstawień:

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

Słowo *kryptografia* szyfrujemy następująco:

k	r	y	p	t	o	g	r	a	f	i	a
N	U	B	T	Y	S	J	U	D	I	L	D

Szyfr Cezara — kryptoanaliza

W celu złamania szyfru Cezara można zastosować następujące techniki:

- sprawdzenie wszystkich kluczy (tzw. atak siłowy, czyli *brute force*),
- w sytuacji, gdy znany jest szyfrogram przynajmniej jednej litery, można wyliczyć klucz (tzw. *atak ze znanym tekstem jawnym*),
- w przypadku długiego klucza można użyć metody *analizy częstotliwości* lub metody *dopasowania histogramu częstości występowania liter*. O tych metodach będziemy mówić dalej.

Szyfr Polibiusza

W II w.p.n.e grecki historyk Polibiusz wymyślił następujący

Algorytm:

Wpisujemy litery alfabetu łacińskiego w kwadratową tablicę wymiaru 5×5 utożsamiając litery *i* oraz *j*.

	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

Tak skonstruowaną tablicę nazywamy *tablicą Polibiusza*.
Każdą literę tekstu jawnego zastępujemy parą liczb, z których pierwsza jest numerem wiersza, a druga numerem kolumny tablicy Polibiusza zawierających daną literę.

Szyfr Polibiusza – przykład

	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

Szyfrogramem słowa *kryptografia* jest

25 42 54 35 44 34 22 42 11 21 24 11.

Uwaga

Szyfr Polibiusza jest „szyfrem bez klucza”, a dokładniej — kodem.

Użyteczna modyfikacja szyfru Polibiusza

- W celu zwiększenia bezpieczeństwa używa się **szyfru Polibiusza z wybranym słowem**.
- Jako *klucz* ustala się dowolne słowo.
- *Algorytm* modyfikuje się następujaco: Litery klucza wpisuje się kolejno wierszami do klatek tablicy Polibiusza pomijając te litery, które w słowie kluczowym powtarzają się. Resztę klatek tablicy wypełnia się kolejnymi, niewykorzystanymi dotychczas, literami alfabetu. Dalej proces szyfrowania przebiega jak poprzednio.

Uwaga

Szyfr Polibiusza jest szyfrem podstawieniowym monoalfabetycznym.

Szyfr Polibiusza z wybranym słowem – przykład

Klucz: *matematyka*

Tablica Polibiusza:

	1	2	3	4	5
1	m	a	t	e	y
2	k	b	c	d	f
3	g	h	i/j	l	n
4	o	p	q	r	s
5	u	v	w	x	z

.

Szyfrogramem słowa *kryptografia* jest

21 44 15 42 13 41 31 44 12 25 33 12.