Kryptologia laboratorium 4.

Atak statystyczny na szyfr monoalfabetyczny

Tomasz Gzella
Instytut Matematyki Stosowanej

WYDZIAŁ FIZYKI TECHNICZNEJ
I MATEMATYKI STOSOWANEJ

POLITECHNIKA
GDAŃSKA

Kilka słów o projekcie

Przykładowa treść sprawozdania projektowego

- opis działania szyfru/maszyny szyfrującej,
- przykłady obliczeniowe,
- krótki rys historyczny,
- próby złamania (historyczne lub własne),
- podział pracy w zespole.

Kilka słów o projekcie

Przykładowa treść sprawozdania projektowego

- opis działania szyfru/maszyny szyfrującej,
- przykłady obliczeniowe,
- krótki rys historyczny,
- próby złamania (historyczne lub własne),
- podział pracy w zespole.

Najważniejsze są wnioski.

Kilka słów o projekcie

Przykładowa treść sprawozdania projektowego

- opis działania szyfru/maszyny szyfrującej,
- przykłady obliczeniowe,
- krótki rys historyczny,
- próby złamania (historyczne lub własne),
- podział pracy w zespole.

Najważniejsze są wnioski.

Trzeba odpowiedzieć na pytania:

- Którymi z tych zadań chcemy się zająć, a którymi nie?

Kilka słów o projekcie

Przykładowa treść sprawozdania projektowego

- opis działania szyfru/maszyny szyfrującej,
- przykłady obliczeniowe,
- krótki rys historyczny,
- próby złamania (historyczne lub własne),
- podział pracy w zespole.

Najważniejsze są wnioski.

Trzeba odpowiedzieć na pytania:

- Którymi z tych zadań chcemy się zająć, a którymi nie?
- Kiedy wspólnie sprawdzimy sprawozdanie i prezentację, by nie składały się z trzech osobnych fragmentów?

Kilka słów o projekcie

Przykładowa treść sprawozdania projektowego

- opis działania szyfru/maszyny szyfrującej,
- przykłady obliczeniowe,
- krótki rys historyczny,
- próby złamania (historyczne lub własne),
- podział pracy w zespole.

Najważniejsze są wnioski.

Trzeba odpowiedzieć na pytania:

- Którymi z tych zadań chcemy się zająć, a którymi nie?
- Kiedy wspólnie sprawdzimy sprawozdanie i prezentację, by nie składały się z trzech osobnych fragmentów?
- Kiedy zrobimy wstępną prezentację?
- Czy każdy będzie mógł odpowiedzieć na pytanie z "nie swojej" części?

Szyfr monoalfabetyczny

Każdej literze alfabetu przyporządkowujemy inną literę alfabetu. Zatem kluczem jest np. 26 znaków alfabetu ustawionych w wybranej kolejności.

Przykład:

a	b	c	d	e	f	g	h	i	j	k	l	m
X	A	Y	D	Z	I	H	G	J	B	O	N	P

n	o	p	q	r	s	t	u	v	w	x	y	z
M	Q	K	R	C	S	U	T	W	L	V	F	E

Szyfr monoalfabetyczny

Każdej literze alfabetu przyporządkowujemy inną literę alfabetu. Zatem kluczem jest np. 26 znaków alfabetu ustawionych w wybranej kolejności.

Przykład:

a	b	c	d	e	f	g	h	i	j	k	l	m
X	A	Y	D	Z	I	H	G	J	B	O	N	P

n	o	p	q	r	s	t	u	v	w	x	y	z
M	Q	K	R	C	S	U	T	W	L	V	F	E

Przykładowy klucz:
xaydzihgjbonpmqkrcsutwlvfe

Atak ze znanym szyfrogramem: atak statystyczny

- **Analiza częstotliwości** (atak statystyczny):
  Polega na wyszukiwaniu często powtarzających się liter i popularnych sekwencji znaków.

  Zależy od języka. Przykładowo możemy łatwo odszukać "częstotliwość występowania liter w języku polskim", o ile mamy podstawy sądzić, że tekst jawny był w języku polskim.

  Dzięki temu atakowi, przy dostatecznie długiej wiadomości, zdołamy odgadnąć większą część klucza.