

Kryptografia

Kryptoanaliza klasyczna

dr Robert Borowiec

Politechnika Wrocławska

Instytut Telekomunikacji i Akustyki

pokój 908, C-5

tel. 3203083

e-mail: robert.borowiec@ita.pwr.wroc.pl

www: lstwww.ita.pwr.wroc.pl/~RB/

Wykład VI

1-godzina

Metody kryptoanalityczne

- Klasyczne:
 - ⇒ Przeszukiwanie całej przestrzeni klucza (*ang. brute force*)
 - ⇒ Przeszukiwanie zredukowanej przestrzeni klucza, inaczej atak słownikowy
 - ⇒ Bazujące na statystyce
 - ⇒ Bazujące na negatywnym wzorcu
- Nowoczesne:
 - ⇒ Metoda różnicowa
 - ⇒ Kluczy powiązanych
 - ⇒ Metoda liniowa
 - ⇒ Różnicowo-liniowa

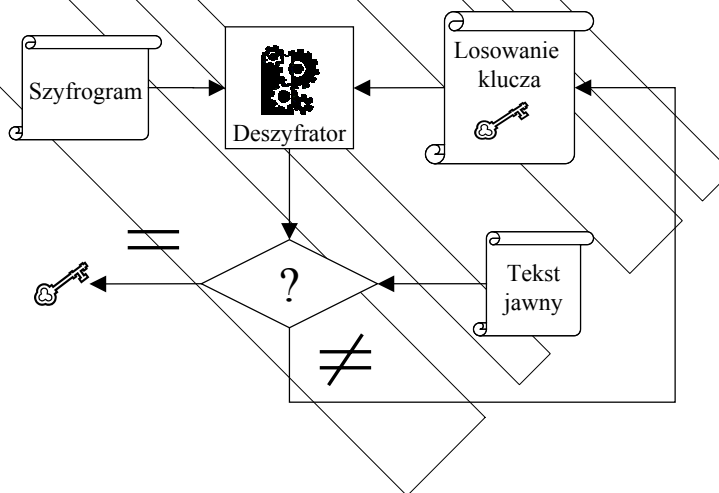
Skuteczna kryptoanaliza

- W celu skutecznej kryptoanalizy musimy uzyskać maksymalną ilość informacji na temat tekstu jawnego:
 - ⇒ rodzaju danych,
 - ⇒ języku,
 - ⇒ kompresji.
- Ponadto pomocne będą informacje na temat:
 - ⇒ metody szyfrowania,
 - ⇒ strony szyfrującej.

Metoda przeszukania całej przestrzeni klucza

- Przeszukanie całej przestrzeni klucza polega na sprawdzeniu każdego możliwego wzorca.
- Skuteczna tylko w przypadku posiadania informacji na temat tekstu jawnego.
- Najskuteczniejsza przy ataku z tekstem jawnym. Wtedy możemy zrobić automat porównujący wzorzec z odszyfrowanym tekstem
- Skuteczna dla małych przestrzeni klucza

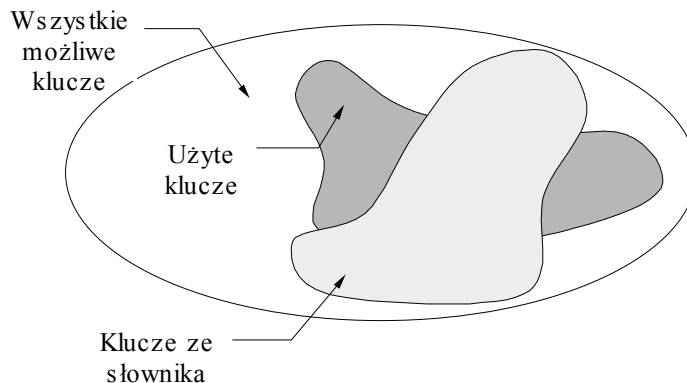
Metoda przeszukania całej przestrzeni klucza (brutal force)



Metoda przeszukania całej przestrzeni klucza (brutal force) cd..

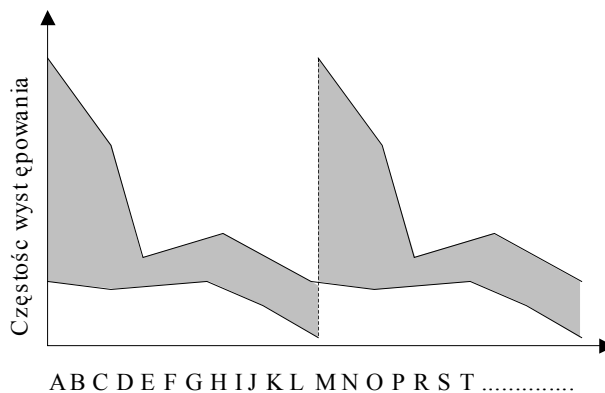
Długość hasła	Tylko litery [26]	Litery duże i małe [52]	Znaki z klawiatury [95]
1	26	52	95
2	676	2704	9 tys.
3	17,5 tys.	140 tys.	857,4 tys.
4	457 tys.	7,3 mln	81,5 mln
5	11,9 mln	380,2 mln	7,7 mld
6	308 mln	19,8 mld	735,1 mld

Atak słownikowy



Metody statystyczne

Metody statystyczne są skuteczne wobec prostych szyfrów opartych na alfabetach przesuniętych.



Koincydencja znaków

Dla dwóch dowolnych tekstów jawnych T_1 i T_2 o równej długości można wyznaczyć współczynnik koincydencji:

$$Kappa = \frac{\text{Liczba znaków zgodnych}}{\text{Liczba znaków w tekście}}$$

$$Kappa = \frac{2}{18}$$

O	t	o		p	i	e	r	w	s	z	y		t	e	k	s	t
a		t	u	t	a	j		m	a	m	y		d	r	u	g	i
												↑	↑				

Standardowo dla odpowiednio długich tekstów $Kappa=9,09\%$

Metoda negatywnego wzorca

PAJPAGOPVWSEANWLNWSZKLKZKXJAOHKSK

PRAWDOPODOBNESŁOWO

PRAWDOPODOBNESŁOWO

PRAWDOPODOBNESŁOWO

PRAWDOPODOBNESŁOWO

> PRAWDOPODOBNESŁOWO

PRAWDOPODOBNESŁOWO

PRAWDOPODOBNESŁOWO

PRAWDOPODOBNESŁOWO

> PRAWDOPODOBNESŁOWO

> PRAWDOPODOBNESŁOWO

PRAWDOPODOBNESŁOWO

PRAWDOPODOBNESŁOWO

> PRAWDOPODOBNESŁOWO

PRAWDOPODOBNESŁOWO

PRAWDOPODOBNESŁOWO

> PRAWDOPODOBNESŁOWO

Łamanie szyfrów okresowych

ustalanie okresu szyfru

➤ Określenie okresu szyfru:

- ⇒ za pomocą wskaźnika zgodności
- ⇒ za pomocą współczynnika koincydencji
- ⇒ metodą Kasiskiego

Wskaźnik zgodności

Wskaźnik zgodności określa prawdopodobieństwo, że dwie litery wybrane losowo z danego kryptogramu będą identyczne

$$WZ = \frac{\sum_{i=0}^{L-1} F_i(F_i - 1)}{N(N - 1)}$$

Dla tekstu w jęz. angielskim

Okres	WZ
1	0,066
2	0,052
3	0,047
4	0,045
5	0,044
10	0,041
Duży	0,038

F_i -częstość wystąpienia i -tego znaku w szyfrogramie

N -długość szyfrogramu

L -długość alfabetu

Wskaźnik koincydencji-Kappa

Kappa kryptogramu przesuniętego o N pozycji i kryptogramu nieprzesuniętego jest równa wartości policzonej analogicznie dla tekstu jawnego.

Kappa będzie największe, gdy wartość przesunięcia N będzie równa okresowi szyfru d .

Dla przesunięć, gdy N jest różne od d , a nawet wielokrotnością d *Kappa* będzie niższa niż dla $N=d$.

Metoda Kasiskiego

- Bazuje na prawdopodobieństwie powtórzenia bloku co najmniej trzech znaków np. (prz, krz, uje).
- jeśli dwa takie same ciągi znaków znajdują się w tekście jawnym w odstępnie równym wielokrotności okresu, to w szyfrogramie uzyskamy identyczny fragment kryptogramu.
- Dla odstępów 24, 54, 18, 29, 66 to okres wynosi 6 lub 2 albo 3
- Okres szyfru wyznaczamy

A series of parallel diagonal lines crossing the slide from the top-left to the bottom-right.

KONIEC

Dziękuję za uwagę