

Kryptografia

Kryptografia 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: istwww.ita.pwr.wroc.pl/~RB/

Wykład V
2-godziny

Rodzaje szyfrów

- Szyfry przestawieniowe
- Szyfry podstawieniowe
 - ⇒ szyfry proste
 - ⇒ szyfry homofoniczne
 - ⇒ wieloalfabetowe
 - ⇒ poligramowe
- Szyfry mieszane (podstawieniowo-przestawieniowe)

Szyfr przestawieniowy

tekst jawny $\xrightarrow{\text{zapis}}$ figura $\xrightarrow{\text{odczyt}}$ szyfrogram

	1	2	3	4	5	6
1	m	a	t	e	m	a
2	t	y	k	a	t	o
3	k	r	ó	l	o	w
4	a	n	a	u	k	x

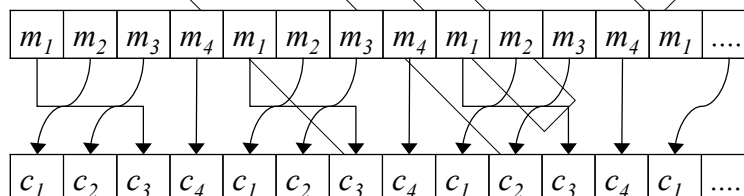
Zapis tekstu jawnego odbywa się wierszami, a odczyt kolumnami. Kluczem kryptograficznym jest długość wiersza, $K=6$

Szyfr przestawieniowy

metoda okresowo-permutacyjna

Informacja jawna $M=m_1m_2\dots m_d m_{d+1}\dots m_{2d}$ dzielona jest na bloki o długości d znaków. Na każdym bloku dokonywane jest przestawienie znaków według określonej funkcji f . Klucz szyfru jest określony się przez $K=(d,f)$.

Przykład: $d=4$; $i=1\ 2\ 3\ 4=d$; $f(i)=2\ 3\ 1\ 4$.



Metoda okresowo permutacyjna

oszacowanie długości krytycznej

- Okres szyfru wynosi $d \Rightarrow$ liczba możliwych przestawień $d!$
- Entropia klucza $H(k) = \log_2 d!$
- Redundancja języka $D = 3.2 \text{ bita/literę}$ (dla języka ang.)
- Przybliżenie Stirlinga: $\log_2 d! \approx d \log_2 \frac{d}{e} + \log_2 \sqrt{2\pi d}$

Krytyczna długość kodu

$$N = \frac{H(k)}{D} = \frac{\log_2 d!}{D} \approx \frac{d \log_2 \frac{d}{e} + \log_2 \sqrt{2\pi d}}{3.2} \approx 0.3 \cdot d \log_2 \frac{d}{e}$$

Szyfr podstawieniowy

monoalfabetyczny

Szyfry podstawieniowe monoalfabetyczne zamieniają znak alfabetu \mathcal{A} określonego dla wiadomości jawnej na znak alfabetu kryptogramu \mathcal{C} .

$$f: \mathcal{A} \rightarrow \mathcal{C}$$

Funkcja f jednoznacznie przyporządkowuje:

\mathcal{A} - alfabet n znakowy dla tekstów jawnych $\{a_1, a_2, \dots, a_n\}$ na

\mathcal{C} - alfabet n znakowy $\{f(a_1), f(a_2), \dots, f(a_n)\}$

Przykład: \mathcal{A} : ABCDEFGHIJKLMNOPQRSTUVWXYZ

\mathcal{C} : HARPSICODBEFGJKLMNQUTUVWXYZ

$$M = \text{KRYPTOGRAFIA} \Rightarrow E_K(M) = \text{ENYLT KCN HIDH}$$

Szyfr podstawieniowy

monoalfabetyczny-przesunięciowy

Jeżeli funkcja f jest funkcją przesunięcia alfabetu o k pozycji to jest to szyfr przesunięciowy i można go zapisać formalnie w postaci:

$$f(a) = (a + k) \bmod n$$

..	X	Y	Z	A	B	C	D	E	..
----	---	---	---	---	---	---	---	---	----

$k=3$

..	X	Y	Z	A	B	C	D	E	..
----	---	---	---	---	---	---	---	---	----

n -jest licznością używanego alfabetu

Szyfr podstawieniowy

inne szyfry oparte na przesunięciu alfabetu

- $f(a) = (a \cdot k) \bmod n$, warunek: $\text{NWD}(k, n) = 1$
- $f(a) = (a \cdot k_1 + k_0) \bmod n$, warunek: $\text{NWD}(k_1, n) = 1$
- $f(a) = (a^t \cdot k_t + a^{t-1} \cdot k_{t-1} + \dots + a^1 \cdot k_1) \bmod n$, warunek: $\text{NWD}(k_p, n) = 1$

gdzie:

NWD-największy wspólny dzielnik,

NWD=1-oznacza, że liczby są względnie pierwsze

Szyfr podstawieniowy

oszacowanie długości krytycznej

Dla alfabetu zawierającej n liter, liczba wszystkich możliwych kluczy wynosi $n!$. W przypadku szyfrów bazujących na przesunięciu alfabetów już tylko n .

Krytyczna długość kodu

$$N = \frac{H(k)}{D} = \frac{\log_2 n!}{D} \approx 28 \quad \text{-dla szyfrów podstawieniowych}$$

$$N = \frac{H(k)}{D} = \frac{\log_2 n}{D} \approx 1.5 \quad \text{-dla szyfrów przesunięciowych}$$

Szyfr podstawieniowy

homofoniczny

Szyfr homofoniczny odzwierciedla każdą literę alfabetu na zbiór homofonów. Litery częściej występujące w tekście mają przydzieloną większą liczbę homofonów.

Litera alfabetu A	Homofony
A	17 19 34 12 ..
B	05 09 11 ..
C	02 06 78 ..
D	04 55 ..
...	...

Szyfr podstawieniowy homofoniczny

Przykład tekstu zaszyfrowanego:

$M: ABBA \Rightarrow C: 17\ 05\ 11\ 12$

- Czym większa liczba homofonów przypadająca na każdy znak alfabetu informacji jawnej tym szyfr jest trudniejszy do przełamania.
- Szyfr homofoniczny może być teoretycznie nieprzełamywalny, gdy zaszyfrowanie każdej litery tekstu jawnego daje w wyniku unikatowy symbol alfabetu szyfrowego
- Szyfr homofoniczny wyższego stopnia umożliwia zawarcie w kryptogramie informacji prawdziwej i nieprawdziwej.

Szyfr podstawieniowy homofoniczny wyższego stopnia

Tworzenie tablicy homofonów

		Klucz k_1			
		→			
Klucz k_2		A	L	M	P
	A	08	15	03	13
	L	01	09	12	06
	M	07	14	02	11
	P	10	04	16	05

Informacja:

$M = \text{LAMP}$ -prawdziwa

$X = \text{PALMA}$ -fałszywa

Kryptogram:

$C = 06\ 08\ 14\ 16\ 08$

Szyfr podstawieniowy wieloalfabetowy

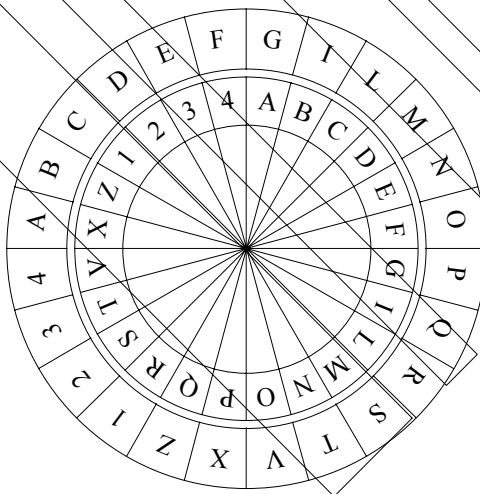
- Ukrywa statystyczne właściwości języka poprzez użycie wielu podstawie
- Szyfry wieloalfabetowe są okresowymi szyframi podstawieniowymi

Mamy dane d alfabetów szyfrowych C_1, C_2, \dots, C_d oraz funkcję

$$f_i : A \rightarrow C_i$$

$$E_k(M) = f_1(m_1)f_2(m_2)\dots f_d(m_d)f_1(m_{d+1})\dots f_d(m_{zd})$$

Szyfr podstawieniowy wieloalfabetowy



Szyfr podstawieniowy

wieloalfabetowy Vignere'a i Beauforta

Klucz szyfru K tworzy sekwencja liter

$$K = k_1 k_2 \dots k_d$$

Gdzie k_i jest liczbą przesunięć w i -tym alfabecie $i=1..d$, tj.:

$$f_i(a) = (a + k_i) \bmod n - \text{Vignere'a}$$

$$f_i(a) = (k_i - a) \bmod n - \text{Beauforta}$$

Tablica Vignere'a

Tekst jawny

	A	B	C	D	E	F	G	H	I	J	K	..	U	V	W	Z	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	..	U	V	W	Z	Y	Z
B	B	C	D	E	F	G	H	I	J	K	..	U	V	W	Z	Y	Z	A
C	C	D	E	F	G	H	I	J	K	..	U	V	W	Z	Y	Z	A	B
D	D	E	F	G	H	I	J	K	..	U	V	W	Z	Y	Z	A	B	C
E	E	F	G	H	I	J	K	..	U	V	W	Z	Y	Z	A	B	C	D
F	F	G	H	I	J	K	..	U	V	W	Z	Y	Z	A	B	C	D	E
G	G	H	I	J	K	..	U	V	W	Z	Y	Z	A	B	C	D	E	F
:	:	:	:	:	:	:	:	:	:	:	:	:	:	:	:	:	:	:
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	..	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	..	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	..	U	V	W	Z
Z	Z	A	B	C	D	E	F	G	H	I	J	K	..	U	V	W	Z	Y

Klucz

Szyfr podstawieniowy wieloalfabetowy

Oszacowanie długości krytycznej

Jeżeli dla pojedynczego podstawienia istnieje s możliwych kluczy (s -długość alfabetu), to przy d -podstawieniach (d -długość klucza) długość krytyczna kryptogramu wynosi:

$$N = \frac{H(k)}{D} = \frac{\log_2 s^d}{D} = \frac{d \log_2 s}{D}$$

Dla $D=3,2$ oraz $s=27$, to długość krytyczna kryptogramu wynosi:

$$N \approx 1,5d$$

Szyfr podstawieniowy z kluczem bieżącym

- Jeżeli do zakodowania informacji o długości L użyty zostanie klucz w postaci ciągu znaków o takiej samej długości, to jest to szyfrowanie z kluczem bieżącym.
- Klucz może stanowić inny tekst, bądź też losowa sekwencja znaków.
- Przy zastosowaniu klucza losowego jednokrotnie i bez powtórzeń, to taki szyfr nazywany jest szyfrem z kluczem jednokrotnym. *Szyfr taki jest bezwarunkowo bezpieczny lub też teoretycznie nieprzełamywalny.*

Szyfr podstawieniowy z kluczem bieżącym implementacja

- Do zaszyfrowania informacji z kluczem bieżącym można użyć tablicy Vinegre'a
- W maszynach cyfrowych częściej stosuje się do tego celu algorytm XOR. Litery alfabetu oraz znaki klucza sumuje się modulo n -ilość znaków w alfabecie.

Przykład:

$M = \text{TO|JEST|SZYFR|Z|KLUCZEM|BIEZACYM}$

$K = \text{TO|JEST|KLUCZ|UZYTY|DO|KODOWANIA}$

$E_k(M) = \text{MCSIKMCKSHQTJNBCSWPLSVAPGM}$

Maszyny rotorowe

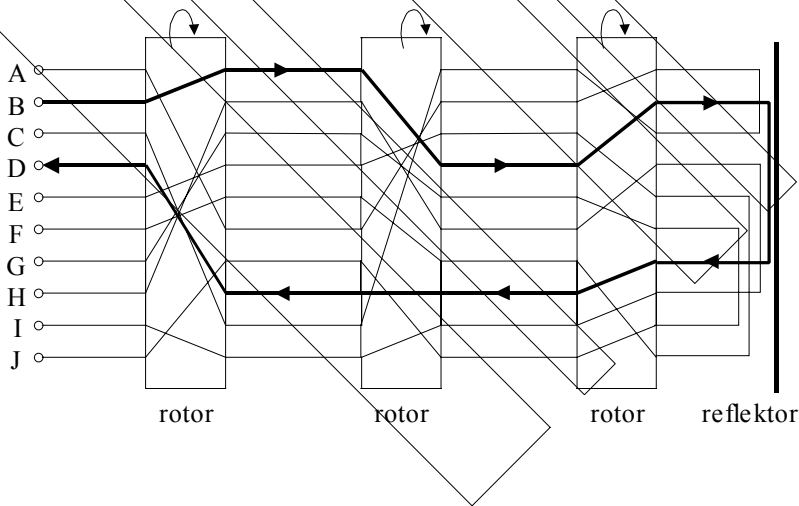
- Maszyny rotorowe można przyrównać do szyfrowania za pomocą dysku szyfrowego. Każdy obrót rotora o jedną pozycję to nowe podstawienie alfabetu
- Funkcja szyfrująca zdefiniowana przez rotor R_i ustawiony w pozycji j_i

$$F_i(a) = (f_i(a - j_i) \bmod 26 + j_i) \bmod 26$$

- Przy t rotorach znak m_i tekstu jawnego jest szyfrowany według zależności

$$E_{k_i}(m_i) = F_t \circ \dots \circ F_1(a)$$

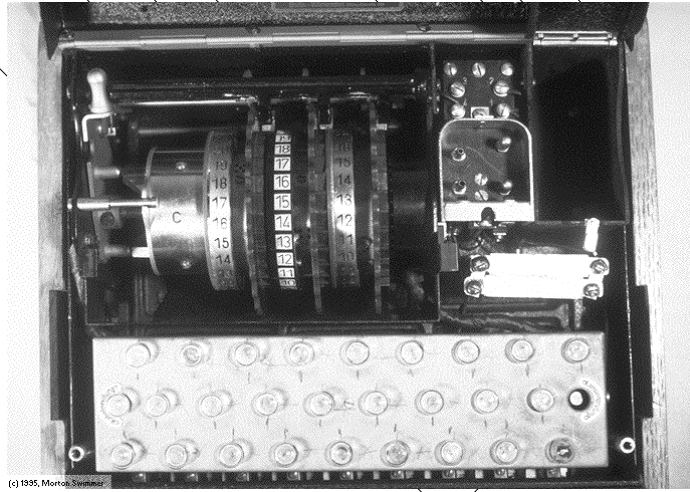
Maszyny rotorowe



Maszyny rotorowe

- Maszyny rotorowe są realizacją szyfrów wieloalfabetowych o długim okresie szyfrowania
- Dla $t=6$ - rotorów z 26 znakami każdy, okres szyfrowania wynosi $26^t=308915776$
- Najpopularniejszą maszyną rotorową była ENIGMA używana przez Niemców oraz jej modyfikacja używana przez Japończyków (kod purpurowy)

ENIGMA



(c) 1995, Mortob-Siemens

Szyfr podstawieniowy poligramowy

- Szyfry poligramowe w jednym kroku dokonują podstawienia większej grupy liter, a nie pojedynczych znaków
- Szyfr taki zamazuje naturalny rozkład częstości występowania liter
- Jako przykład szyfru poligramowego jest szyfr Playfaira. Zastępuje on zestawy dwuliterowe sekwencjami dwuliterowymi

Szyfr poligramowy Playfaira

Do kodowania używana była tablica 5×5 znaków (bez litery j)

H	A	R	P	S
I	C	O	D	B
E	F	G	K	L
M	N	Q	T	U
V	W	X	Y	Z

- Jeśli obydwa znaki m_1 i m_2 z analizowanego diagramu są w tym samym wierszu macierzy, to c_1 i c_2 są znakami kryptogramu odczytywanymi z prawej strony m_1 i m_2 macierzy. Prawa strona ostatniej kolumny to pierwsza z lewej.
- Jeśli obydwa znaki m_1 i m_2 z analizowanego diagramu leżą w tej samej kolumnie macierzy, to c_1 i c_2 są znakami kryptogramu odczytywanymi poniżej m_1 i m_2 macierzy. Pierwszy wiersz leży pod ostatnią kolumną.
- Jeśli m_1 i m_2 znajdują się w różnych wierszach i kolumnach to c_1 i c_2 są brane z przeciwległych rogów prostokąta wyznaczonego przez m_1 i m_2 , przy czym c_1 pochodzi z wiersza zawierającego m_1 , c_2 zaś z wiersza zawierającego m_2 .
- Jeśli $m_1 = m_2$ to do tekstu jawnego pomiędzy te litery wstawia się nieznaczającą literę np.. X, co eliminuje powtórzenia.

KONIEC

Dziękuję za uwagę