Bezpieczeństwo systemów komputerowych

Algorytmy kryptograficzne (1)

mgr Katarzyna Trybicka-Francik
kasiat@zeus.polsl.gliwice.pl
pok. 503

Algorytmy kryptograficzne

- Przestawieniowe
  zmieniają porządek znaków według pewnego schematu, tzw. figury
- Podstawieniowe
  - monoalfabetyczne
  - homofoniczne
  - wieloalfabetowe
  - poligramowe

Algorytmy kryptograficzne

- Przestawieniowe
  zmieniają porządek znaków według pewnego schematu, tzw. figury
- Podstawieniowe
  - monoalfabetyczne
  - homofoniczne
  - wieloalfabetowe
  - poligramowe

Szyfry przestawieniowe

- Przestawienie kolumnowe

Przykład.
tekst jawny: KRYPTOGRAFIA
macierz: 3x4
klucz: 2-4-1-3

1	2	3	4
K	R	Y	P
T	O	G	R
A	F	I	A

tekst zaszyfrowany:
ROFPRAKTAYGI

BSK - 2003 Copyright by K. Trybicka-Francik

Szyfry przestawieniowe

- Stałego okresu d

Przykład.
tekst jawny: KRYPTOGRAFIA
klucz K=(d, f) : d=4,
i: 1 2 3 4
f(i): 2 4 1 3

KRYP TOGR AFIA
RPKY ORTG FAAI

tekst zaszyfrowany:
RPKYORTGFAAI

BSK - 2003 Copyright by K. Trybicka-Francik

Szyfry przestawieniowe

- Szyfry przestawieniowe

Szyfr płotkowy

tekst jawny: KRYPTOGRAFIA
klucz K=(d) : d=3

tekst zaszyfrowany:
KTARPORFAYGI

KRYPTOGRAFIA
K T A
R P O R F A
Y G I
KTARPORFAYGI

BSK - 2003 Copyright by K. Trybicka-Francik

Algorytmy kryptograficzne

- Przestawieniowe
  zmieniają porządek znaków według pewnego schematu, tzw. figury
- Podstawieniowe
  - monoalfabetyczne
  - homofoniczne
  - wieloalfabetowe
  - poligramowe

BSK - 2003 Copyright by K. Trybicka-Francik

Szyfry podstawieniowe

- Szyfr monoalfabetyczny
  zamienia każdy znak uporządkowanego alfabetu jawnego A na odpowiedni znak uporządkowanego alfabetu szyfru C

Przekład.

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

KRYPTOGRAFIA
ENYLTKCNHIDH

BSK - 2003 Copyright by K. Trybicka-Francik

Szyfry podstawieniowe

- Szyfr monoalfabetyczny

Przekład. Szyfr cmentarny

A•	B•	C•
D•	E•	F•
G•	H•	IJ•

K:	L:	M:
N:	O:	P:
Q:	R:	S:

T	U	V
W	X	Y
Z		

KRYPTOANALIZA

BSK - 2003 Copyright by K. Trybicka-Francik

Szyfry podstawieniowe

- Homofoniczne
  odwzorowuje każdy znak „a" alfabetu tekstu jawnego na zestaw elementów f(a) tekstu zaszyfrowanego, zwanych homofonami.

Szyfry podstawieniowe

- Homofoniczne

Przykład.

tekst jawny: ANALIZA

litera	homofony
A	17 19 34 41 56 60 67 83
I	08 22 53 65 88 90
L	03 44 76
N	02 09 15 27 32 40 59
Z	01 11 23 28 42 54 70 80

tekst zaszyfrowany:

17 32 60 44 88 23 41

Szyfry podstawieniowe

- Homofoniczne wyższego stopnia

Przykład.
macierz: 5x5
tekst jawny: LALKA
tekst fałszywy: KAJAK

M = L A L K A
X = K A J A K

	A	I	J	K	L
A	10	22	18	02	11
I	12	01	25	05	20
J	19	06	23	13	07
K	03	16	08	24	15
L	17	09	21	14	04

14 10 21 03 02 szyfrogram

Szyfry podstawieniowe

- Wieloalfabetowe

Przykład. Szyfr Vigenerè'a
tekst jawny: LEKKOATLETKA
klucz: CZAD

M = LEKKOATLETKA
K = CZADCZADCZAD

NDKNQZTOGS szyfrogram

	A	B	C	D	E	F	G	H	I	J	K	L...
A	A	B	C	D	E	F	G	H	I	J	K	L...
B	B	C	D	E	F	G	H	I	J	K	L	M...
C	C	D	E	F	G	H	I	J	K	L	M	N...
D	D	E	F	G	H	I	J	K	L	M	N	O...
...												
Z	Z	A	B	C	D	E	F	G	H	I	J	K ...

Szyfry podstawieniowe

- Polimorficzne

szyfrują w jednym kroku większą grupę liter.

Przykład. Szyfr Playfaira

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**

Szyfry podstawieniowe

1. Jeśli m_1 i m_2 znajdują się w tym samym wierszu, to c_1 i c_2 są znakami z prawej strony m_1 i m_2, przy czym pierwszą kolumnę traktuje się jako położoną na prawo od ostatniej kolumny.
2. Jeśli m_1 i m_2 znajdują się w tej samej kolumnie, to c_1 i c_2 są znakami położonymi poniżej m_1 i m_2, przy czym pierwszy wiersz traktuje się jako leżący pod ostatnim wierszem.
3. Jeśli m_1 i m_2 znajduje 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 $m_{2.}$
4. Jeśli $m_1 = m_2$, to do tekstu jawnego między te litery wstawia się nieznaczącą literę (np. X), co eliminuje powtórzenia.
5. Jeśli tekst jawny ma nieparzystą liczbę znaków, to na końcu tekstu jawnego dopisuje się nieznaczącą literę.

Szyfry podstawieniowe

- Szyfry podstawieniowe

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

KR YP TO GR AF IA
GP PD QD QO CN CH

BSK - 2003 Copyright by K. Trybicka-Francik

Bezpieczeństwo systemów komputerowych

Zaawansowane algorytmy kryptograficzne

mgr Katarzyna Trybicka-Francik
kasiat@zeus.polsl.gliwice.pl
pok. 503

Klasyfikacja

- Szyfry blokowe
- Szyfry strumieniowe

BSK - 2003 Copyright by K. Trybicka-Francik

Szyfry blokowe

- Działają na blokach informacji, tekstu jawnego, lub szyfrogramu (zwykle 64 bity).
- Nie pracują „bezobsługowo”.
- Są bardzo funkcjonalne.
- Pracują w różnych trybach.

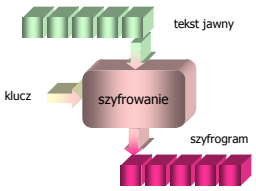
Szyfry blokowe

Tryby pracy

- Tryb elektronicznej książki kodowej (electronic codebook).
- Tryb wiązania bloków zaszyfrowanych (cipher block chaining).
- Tryb sprzężenia zwrotnego szyfrogramu (cipher feedback).
- Tryb sprzężenia zwrotnego wyjściowego (output feedback).

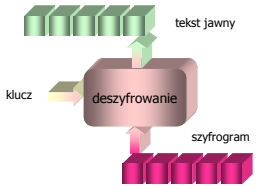
Tryby pracy

Tryb elektronicznej książki kodowej (electronic codebook)



Tryby pracy

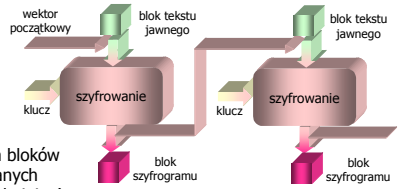
Tryb elektronicznej książki kodowej (electronic codebook)



Tryb elektronicznej książki kodowej

- ZALETY
  - Najłatwiejszy i najszybszy tryb pracy
  - Możliwość niezależnego szyfrowania każdego bloku tekstu (bazy danych)
  - Propagacja błędu
- WADY
  - Podatny na ataki

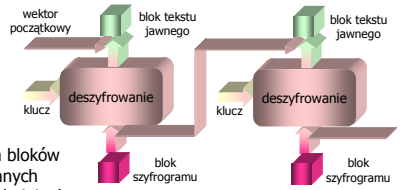
Tryby pracy



Tryb wiązania bloków zaszyfrowanych (cipher block chaining)

BSK - 2003 Copyright by K. Trybicka-Francik

Tryby pracy



Tryb wiązania bloków zaszyfrowanych (cipher block chaining)

BSK - 2003 Copyright by K. Trybicka-Francik

Tryb wiązania bloków zaszyfrowanych

Tekst jawny jest przed zaszyfrowaniem sumowany mod 2 z poprzednim blokiem szyfrogramu.

Szyfrowanie:

$$C_i = E_k (P_i \oplus C_{i-1})$$

Deszyfrowanie:

$$P_i = C_{i-1} \oplus D_K (C_i)$$

BSK - 2003 Copyright by K. Trybicka-Francik

Tryb wiązania bloków zaszyfrowanych

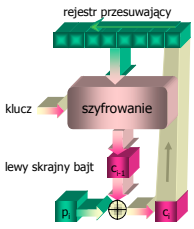
- Wektor początkowy
  - Może być dobierany losowo
  - Nie trzeba go utajniać, może być przesyłany wraz z szyfrogramem
- Błędy
  - Propagacja błędu
  - Błąd w szyfrogramie
  - Błąd synchronizacji

Tryb wiązania bloków zaszyfrowanych

- Nie można zacząć szyfrowania, zanim nie odbierze się całego bloku danych
- Nieprzydatny jeżeli dane muszą być przetwarzane w porcjach wielkości bajtu

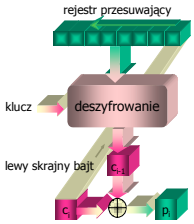
Tryby pracy

Tryb sprzężenia zwrotnego szyfrogramu (cipher feedback).



Tryby pracy

Tryb sprzężenia zwrotnego szyfrogramu (cipher feedback).

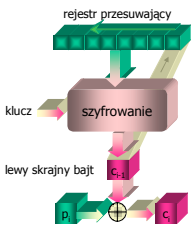


Tryby sprzężenia zwrotnego szyfrogramu

- Propagacja błędu
- Samoodtwarzanie
- Pozwala na szyfrowanie informacji w jednostkach mniejszych niż rozmiar bloku
- Jest wolniejszy od swoich poprzedników

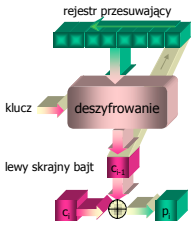
Tryby pracy

Tryb sprzężenia zwrotnego wyjściowego (output feedback)



Tryby pracy

Tryb sprzężenia zwrotnego wyjściowego (output feedback)

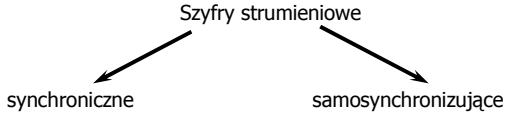


Który do czego?

- Tryb elektronicznej książki kodowej (ECB)
  – bazy danych
- Tryb wiązania bloków zaszyfrowanych (CBC)
  – szyfrowanie plików
- Tryb sprzężenia zwrotnego szyfrogramu (CFB)
  – szyfrowanie strumieni znaków
- Tryb sprzężenia zwrotnego wyjściowego (OFB)
  – w systemach z transmisją synchroniczną o dużej szybkości, bez tolerancji na propagację błędu

Szyfry strumieniowe

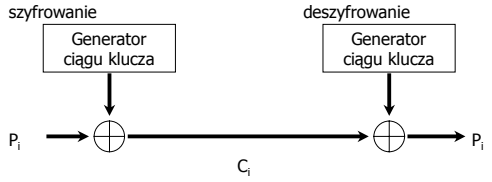
- Szyfrowanie
  $E_K(M) = E_{k1}(m_1)|| E_{k2}(m_2)|| E_{k3}(m_3)||... ||E_{kn}(m_n)$
- Bezpieczeństwo zależy od generatora kluczy



Synchroniczne szyfry strumieniowe

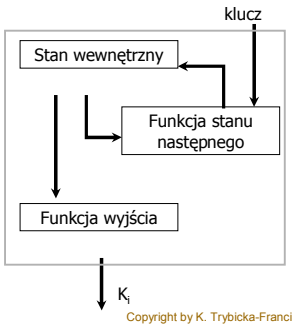
- Klucz generowany niezależnie od strumienia wiadomości
- Po obu stronach, szyfrującej i deszyfrującej generatory strumienia kluczy
- Nie rozsiewają błędów transmisji

Synchroniczne szyfry strumieniowe



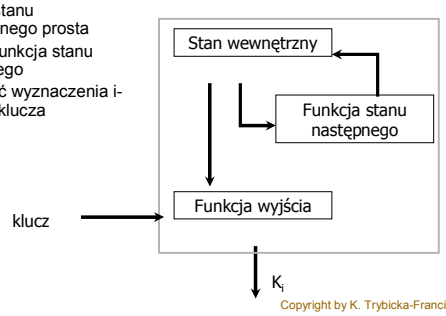
Tryb sprzężenia zwrotnego wyjściowego

- Klucz wpływa na funkcję następnego stanu
- Funkcja wyjściowa nie jest zależna od klucza i zwykle jest bardzo prosta
- Złożoność kryptograficzna spoczywa na funkcji stanu następnego zależnego od niej klucza



Tryb licznikowy

- Funkcja stanu wewnętrznego prosta
- Złożona funkcja stanu wyjściowego
- Możliwość wyznaczenia i-tego bitu klucza



Atak wstawieniowy

- Przechwycenie szyfrogramu
  - t.j. $p_1, p_2, p_3, p_4,\ldots$
  - k $k_1, k_2, k_3, k_4,\ldots$
  - t.z. $c_1, c_2, c_3, c_4,\ldots$
- Wprowadzenie zaburzenia
  - t.j. $p_1, p', p_2, p_3, \ldots$
  - k $k_1, k_2, k_3, k_4,\ldots$
  - t.z. $c_1, c_2', c_3', c_4',\ldots$

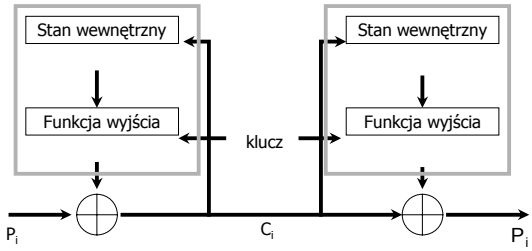
Atak wstawieniowy

- Znając p′ możemy wyznaczyć cały tekst za tym bitem
  - $k_2 = c_2' \oplus p' \quad \Rightarrow \quad p_2 = c_2 \oplus k_2$
  - $k_3 = c_3' \oplus p_2 \quad \Rightarrow \quad p_3 = c_3 \oplus k_3$
  - $k_4 = c_4' \oplus p_3 \quad \Rightarrow \quad p_4 = c_4 \oplus k_4$

Samosynchronizujące szyfry strumieniowe

- Każdy bit ciągu szyfrującego jest funkcją pewnej stałej liczby poprzednich bitów szyfrogramu
- Zwykle pracuje w trybie sprzężenia zwrotnego szyfrogramu

Samosynchronizujące szyfry strumieniowe



Porównanie

Szyfry blokowe

- Łatwe w implementacji
- Silne w działaniu
- Doskonałe do odczytu i zapisu danych w postaci bloku

Szyfry strumieniowe

- Trudne w implementacji programowej
- Łatwe do analizy matematycznej
- Przesył szyfrowanej informacji z terminala

Klucze

- Klucze tajne
- Klucze jawne

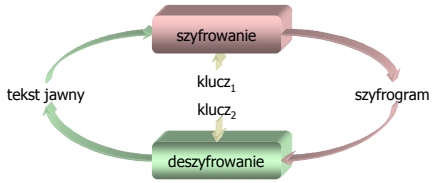
Klucze

- Klucze tajne

Szyfry symetryczne

Klucze

- Klucze jawne



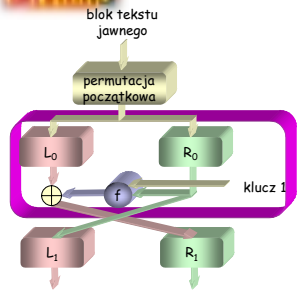
Szyfry asymetryczne

Szyfry podstawieniowo-permutacyjne

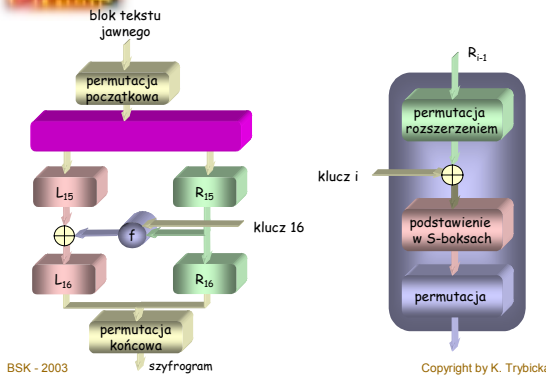
DES (Data Encryption Standard)

- Standard od 23 listopada 1976
- Szyfr blokowy (blok: 64 bity)
- Szyfr symetryczny (klucz: 56 bity)
- Składa się z 16 cykli

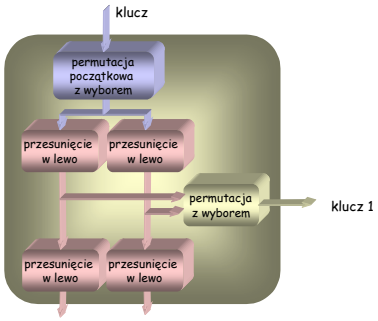
DES (Data Encryption Standard)



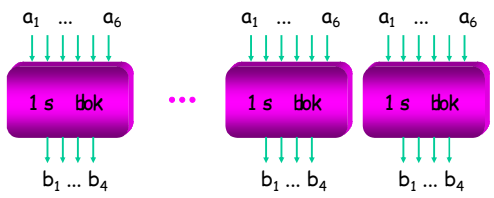
DES (Data Encryption Standard)



DES (Data Encryption Standard)



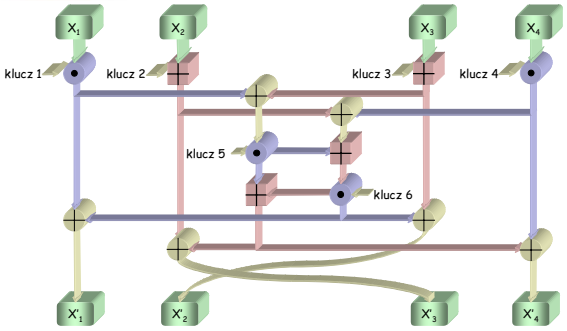
DES (Data Encryption Standard)



IDEA
(International Data Encryption Algorithm)

- Opublikowany 1992
- Szyfr blokowy (blok: 64 bity)
- Szyfr symetryczny (klucz: 128 bity)
- Składa się z 8 cykli

IDEA
(International Data Encryption Algorithm)



IDEA
(International Data Encryption Algorithm)

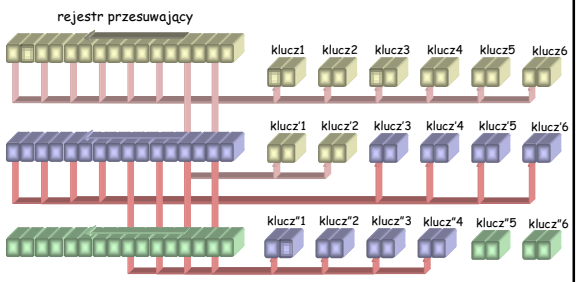
mnożenie liczb ab mod 2^{16} +1 =
(ab mod 2^{16}) (ab div 2^{16})
gdy (ab mod 2^{16})≥(ab div 2^{16})

(ab mod 2^{16}) (ab div 2^{16})+ 2^{16}+1
gdy (ab mod 2^{16})<(ab div 2^{16})

dodawanie mod 2^{16} +1

dodawanie mod 2

IDEA
(International Data Encryption Algorithm)



BSK - 2003 Copyright by K. Trybicka-Francik

Rijndael – AES
(Advanced Encryption Standard)

Opis algorytmu na stronie WWW

BSK - 2003 Copyright by K. Trybicka-Francik

Dziękuję za uwagę

BSK - 2003 Copyright by K. Trybicka-Francik