

Kryptografia

Algorytmy symetryczne

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 VII

2-godziny

Duże liczby

| | |
|--|---------------------------|
| Wiek naszej planety | 2^{30} lat = 2^{55} s |
| Wiek wszechświata | 2^{34} lat = 2^{59} s |
| Liczba atomów w planecie | 2^{170} sztuk |
| Liczba atomów w Słońcu | 2^{190} sztuk |
| Liczba atomów w galaktyce | 2^{223} sztuk |
| Liczba atomów we wszechświecie (łącznie z „czarną materią”) | 2^{265} sztuk |
| Objętość wszechświata | 2^{280} cm ³ |

Najważniejsze znane algorytmy symetryczne

- DES (*ang. Data Encryption Standard*)
- AES (*ang. Advanced Encryption Standard*)-od 2001 roku nowy standard szyfrowania informacji poufnych
- IDEA (*ang. International Data Encryption Algorithm*)

Inne znane algorytmy symetryczne

- Lucifer
- Madrygi
- NewDes
- Feal-N
- Redoc
- Loki
- Khuru i Khafre
- MMB
- CA-1.1
- RC-2
- RC-3
- RC-5
- SAFER
- SkipJack

Algorytm DES

ang. Data Encryption Standard

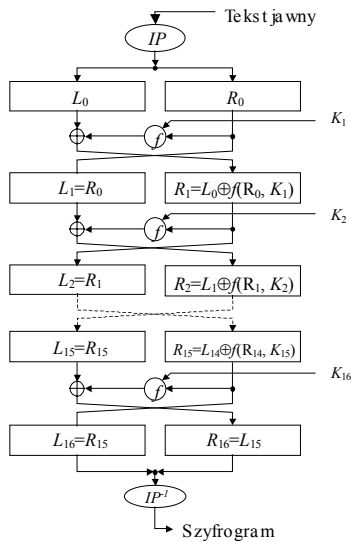
- W 1977 r Narodowe Biuro Normalizacji USA przyjęło standard szyfrowania danych.
- Algorytm szyfrowania informacji DES powstał w firmie IBM i jest rozwinięciem szyfru LUCIFER.
- Algorytm ma zastosowanie do przesyłania informacji poufnych. Szyfr Lucifer, protoplasta szyfru DES pracował z kluczem 128 bitowym. W standardzie DES przyjęto efektywny klucz 56 bitowy.

Algorytm DES

ang. Data Encryption Standard

- Jest to szyfr blokowy wykonujący operacje podstawienia oraz permutacje na 64 bitowych blokach danych wejściowych.
- Algorytm służy do szyfrowania jak i deszyfrowania informacji. Zmienia się tylko kolejność podkluczy.
- Do szyfrowania informacji używa się 16 podkluczy 48 bitowych, które są generowane na podstawie 64 bitowego klucza wejściowego. Przy czym efektywny klucz jest 56 bitowy, gdyż co 8 bit klucza wejściowego jest bitem parzystości.

Ogólny schemat blokowy algorytmu



© Robert Borowiec

Algorytm rozpoczyna się permutacją wstępną IP. Ponieważ algorytm ma być symetryczny, kończy się permutacją odwrotną.

Taka budowa algorytmu umożliwia stosowanie go zarazem do szyfrowania i deszyfrowania informacji. Z tym, że przy deszyfrowaniu informacji kolejność podkluczy jest odwrotna.

Kryptografia, Wykład VII Strona7/42

Tabela permutacji początkowej i końcowej

Tabela permutacji początkowej IP

| IP | | | | | | | |
|----|----|----|----|----|----|----|---|
| 58 | 50 | 42 | 34 | 26 | 18 | 10 | 2 |
| 60 | 52 | 44 | 36 | 28 | 20 | 12 | 4 |
| 62 | 54 | 46 | 38 | 30 | 22 | 14 | 6 |
| 64 | 56 | 48 | 40 | 32 | 24 | 16 | 8 |
| 57 | 49 | 41 | 33 | 25 | 17 | 9 | 1 |
| 59 | 51 | 43 | 35 | 27 | 19 | 11 | 3 |
| 61 | 53 | 45 | 37 | 29 | 21 | 13 | 5 |
| 63 | 55 | 47 | 39 | 31 | 23 | 15 | 7 |

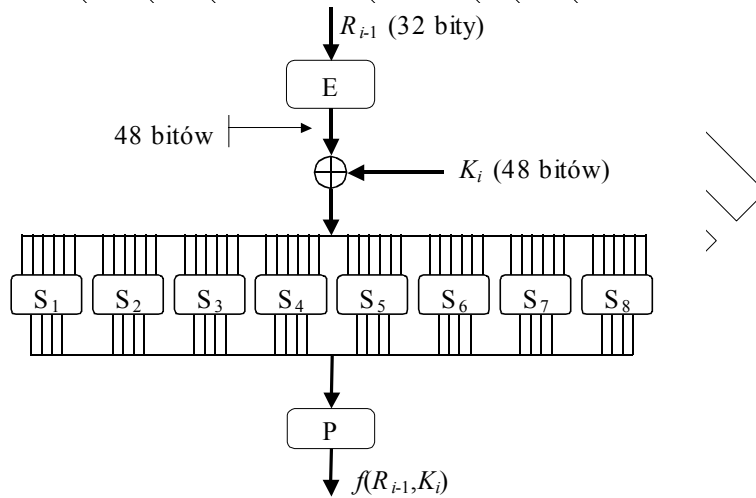
Tabela permutacji końcowej IP^{-1}

| IP | | | | | | | |
|----|---|----|----|----|----|----|----|
| 40 | 8 | 48 | 16 | 56 | 24 | 64 | 32 |
| 39 | 7 | 47 | 15 | 55 | 23 | 63 | 31 |
| 38 | 6 | 46 | 14 | 54 | 22 | 62 | 30 |
| 37 | 5 | 45 | 13 | 53 | 21 | 61 | 29 |
| 36 | 4 | 44 | 12 | 52 | 20 | 60 | 28 |
| 35 | 3 | 43 | 11 | 51 | 19 | 59 | 27 |
| 34 | 2 | 42 | 10 | 50 | 18 | 58 | 26 |
| 33 | 1 | 41 | 9 | 49 | 17 | 57 | 25 |

© Robert Borowiec

Kryptografia, Wykład VII Strona8/42

Obliczanie funkcji $f(R_{i-1}, K_i)$



S-bloki

- S-bloki (*ang. substitution boxes*) dokonują operacji podstawienia nieliniowego.
- Na wejście wprowadzane są bloki 6 bitowe, a na wyjściu pojawiają się bloki 4 bitowe.
- S bloki nie są liniowymi funkcjami afijnymi swojego wejścia, tzn. nie można ułożyć układu równań, z których można wyliczyć bity wyjściowe na podstawie bitów wejściowych.
- Zmiana jednego bitu wejściowego powoduje zmianę co najmniej 2 bitów wyjściowych.
- Minimalizowana jest różnica ilości występowania zer i jedynek.

Tablica stanów dla S-bloku nr 1

(każdy S-blok ma inaczej zdefiniowaną tablicę !!)

| | | $b_2b_3b_4b_5 \rightarrow$ | | | | | | | | | | | | | | | |
|------------------------|------|----------------------------|------|------|------|------|------|------|------|------|------|------|------|------|------|------|------|
| $\leftarrow a_1a_2a_3$ | | 0000 | 0001 | 0010 | 0011 | 0100 | 0101 | 0110 | 0111 | 1000 | 1001 | 1010 | 1011 | 1100 | 1101 | 1110 | 1111 |
| | | (0) | (1) | (2) | (3) | (4) | (5) | (6) | (7) | (8) | (9) | (10) | (11) | (12) | (13) | (14) | (15) |
| | 0000 | 1110 | 0100 | 1101 | 0001 | 0010 | 1111 | 1011 | 1000 | 0011 | 1010 | 0110 | 1100 | 0101 | 1001 | 0000 | 0111 |
| | (0) | (14) | (4) | (13) | (1) | (2) | (15) | (11) | (8) | (3) | (10) | (6) | (12) | (5) | (9) | (0) | (7) |
| | 0001 | 0000 | 1111 | 0111 | 0100 | 1110 | 0010 | 1101 | 0001 | 1010 | 0110 | 1100 | 1011 | 1001 | 0101 | 0011 | 1000 |
| | (1) | (0) | (15) | (7) | (4) | (14) | (2) | (13) | (1) | (10) | (6) | (12) | (11) | (9) | (5) | (3) | (8) |
| | 0010 | 0100 | 0001 | 1110 | 1000 | 1101 | 0110 | 0010 | 1011 | 1111 | 1100 | 1001 | 0111 | 0011 | 1010 | 0101 | 0000 |
| | (2) | (4) | (1) | (14) | (8) | (13) | (6) | (2) | (11) | (15) | (12) | (9) | (7) | (3) | (10) | (5) | (0) |
| | 0011 | 1111 | 1100 | 1000 | 0010 | 0100 | 1001 | 0001 | 0111 | 0101 | 1011 | 0011 | 1110 | 1010 | 0000 | 0110 | 1101 |
| | (3) | (15) | (12) | (8) | (2) | (4) | (9) | (1) | (7) | (5) | (11) | (3) | (14) | (10) | (0) | (6) | (13) |

Tablica wyboru E i permutacji P

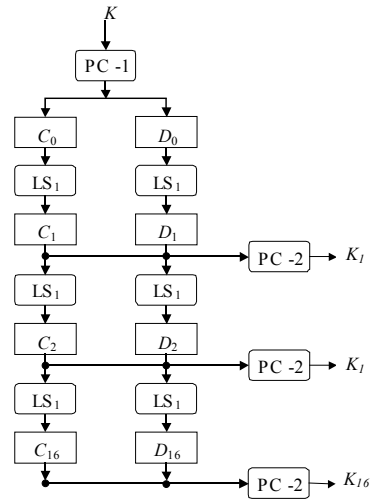
Tablica E wyboru bitów

| | | | | | |
|----|----|----|----|----|----|
| 32 | 1 | 2 | 3 | 4 | 5 |
| 4 | 5 | 6 | 7 | 8 | 9 |
| 8 | 9 | 10 | 11 | 12 | 13 |
| 12 | 13 | 14 | 15 | 16 | 17 |
| 16 | 17 | 18 | 19 | 20 | 21 |
| 20 | 21 | 22 | 23 | 24 | 25 |
| 24 | 25 | 26 | 27 | 28 | 29 |
| 28 | 29 | 30 | 31 | 32 | 1 |

Tablica permutacji P

| | | | |
|----|----|----|----|
| 16 | 7 | 20 | 21 |
| 29 | 12 | 28 | 17 |
| 1 | 15 | 23 | 26 |
| 5 | 18 | 31 | 10 |
| 2 | 8 | 24 | 14 |
| 32 | 27 | 3 | 9 |
| 19 | 13 | 30 | 6 |
| 22 | 11 | 4 | 25 |

Tworzenie kluczy



1. Początkowo klucz jest redukowany z 64 bitów do 56 poprzez odrzucenie bitów parzystości i.
2. Z klucza 56 bitowego tworzone jest 16 różnych kluczy 48 bitowych, które są używane w kolejnych cyklach szyfrowania.

Tworzenie kluczy

Tablica permutacji
klucza PC-1

| | | | | | | |
|----|----|----|----|----|----|----|
| 57 | 49 | 41 | 33 | 25 | 17 | 9 |
| 1 | 58 | 50 | 42 | 34 | 26 | 18 |
| 10 | 2 | 59 | 51 | 43 | 35 | 27 |
| 19 | 11 | 3 | 60 | 52 | 44 | 36 |
| 63 | 55 | 47 | 39 | 31 | 23 | 15 |
| 7 | 62 | 54 | 46 | 38 | 30 | 22 |
| 14 | 6 | 61 | 53 | 45 | 37 | 29 |
| 21 | 13 | 5 | 28 | 20 | 12 | 4 |

Tablica permutacji
klucza PC-2

| | | | | | |
|----|----|----|----|----|----|
| 14 | 17 | 11 | 24 | 1 | 5 |
| 3 | 28 | 15 | 6 | 21 | 10 |
| 23 | 19 | 12 | 4 | 26 | 8 |
| 16 | 7 | 27 | 20 | 13 | 2 |
| 41 | 52 | 31 | 37 | 47 | 55 |
| 30 | 40 | 51 | 45 | 33 | 48 |
| 44 | 49 | 39 | 56 | 34 | 53 |
| 46 | 42 | 50 | 36 | 29 | 32 |

Ilość przesunięć połówek klucza C i D

| | | | | | | | | | | | | | | | | |
|----|---|---|---|---|---|---|---|---|---|----|----|----|----|----|----|----|
| I | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |
| LS | 1 | 1 | 2 | 2 | 2 | 2 | 2 | 2 | 1 | 2 | 2 | 2 | 2 | 2 | 2 | 1 |

Klucze słabe w DES

Z powodu sposobu generowania podkluczy w systemie DES, istnieją:

- *4-klucze słabe*
- *12-kluczy półsłabych*

Klucze słabe - podklucze generowane w kolejnych cyklach z kluczy słabych są identyczne.

Klucze półsłabe - generują tylko dwa różne podklucze zamiast 16 różnych. Tak więc każdy podklucz jest używany w algorytmie 8 razy.

Wydajność

- Algorytm DES został zaimplementowany w postaci programowej oraz sprzętowej
 - ⇒ *Prędkość szyfrowania za pomocą układów sprzętowych wynosi 1 GBit/s (dane z 1985 r).*
 - ⇒ *Najszybsze implementacje programowe osiągnęły prędkość 14 MBit/s. (dane z 2000 roku)*

Opublikowane metody łamania szyfrów

1. Metoda siłowa -(*ang. brutal force*)
przeszukiwanie całej przestrzeni klucza
2. Kryptoanaliza różnicowa
3. Kryptoanaliza metodą kluczy powiązanych
4. Kryptoanaliza liniowa

Wyniki kryptoanalizy DES

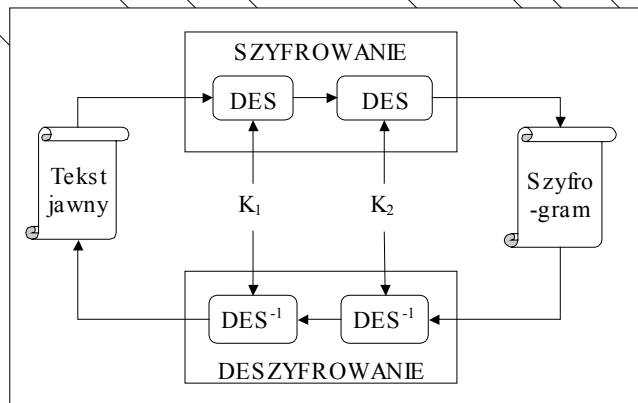
| Rodzaj kryptoanalizy | Wybrane teksty jawne | Znane teksty jawne | Analizowane teksty jawne | Złożoność obliczeniowa |
|----------------------|----------------------|----------------------|--------------------------|------------------------|
| Brutalna | 1 | 1 (8 Bajtów) | 1 | 2^{56} |
| Różnicowa | 2^{47} | 2^{55} (262144 TB) | 2^{36} | 2^{37} |
| Kluczy powiązanych | 2^{17*} | 2^{33*} (64 MB) | b.d. | b.d. |
| Liniowa | b.d. | 2^{47} (1024 TB) | b.d. | b.d. |

* znana jest różnica pomiędzy dwoma kluczami

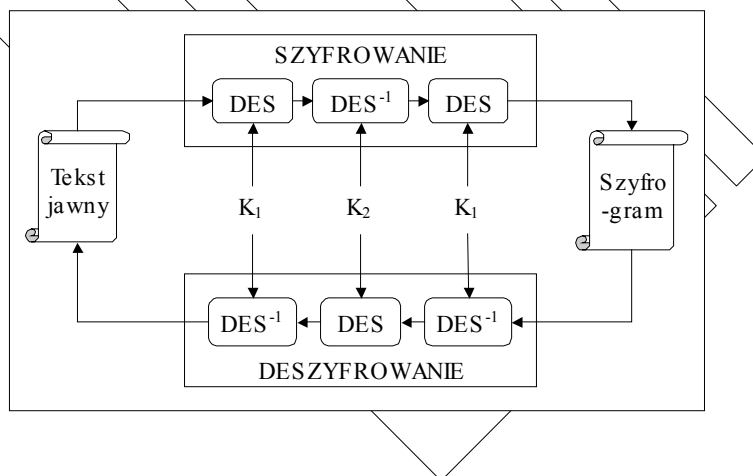
Kryptoanaliza algorytmu DES

- Według opinii kryptoanalityków z roku 1985 klucz 56 bitowy był za krótki. Nie zapewniał on bowiem odpowiedniego poziomu bezpieczeństwa.
- Szyfr DES można bowiem złamać przy ataku brutalnym (*przeszukanie całej przestrzeni klucza*) z *tekstem jawnym* w ciągu jednego dnia przy zastosowaniu maszyny złożonej z 1 miliona procesorów i sprawdzającej jeden klucz w ciągu 1 μ s.
- W końcu lat 90 złamano metodą brutalną szyfr DES z kluczem 56 bitowym w ciągu 3 dni na specjalizowanej maszynie liczącej, po przeszukaniu 1/3 kluczy. Wynika z tego, że każdy szyfrogram DES na tej maszynie można złamać w ciągu 9 dni.

Podwójny DES



Potrójny DES



Narodziny standardu AES

- We wrześniu 1997 roku NIST (*ang. National Institute of Standards and Technology*) ogłosił konkurs na nowy system szyfrujący, który ma spełniać określone założenia.
- W listopadzie 2001 roku NIST (*ang. National Institute of Standards and Technology*) przyjął nowy standard szyfrowania danych AES.
- Do szyfrowania w nowym standardzie został wybrany algorytm *Rijndael* (autorstwa Joan Daemen i Vincent Rijmen)

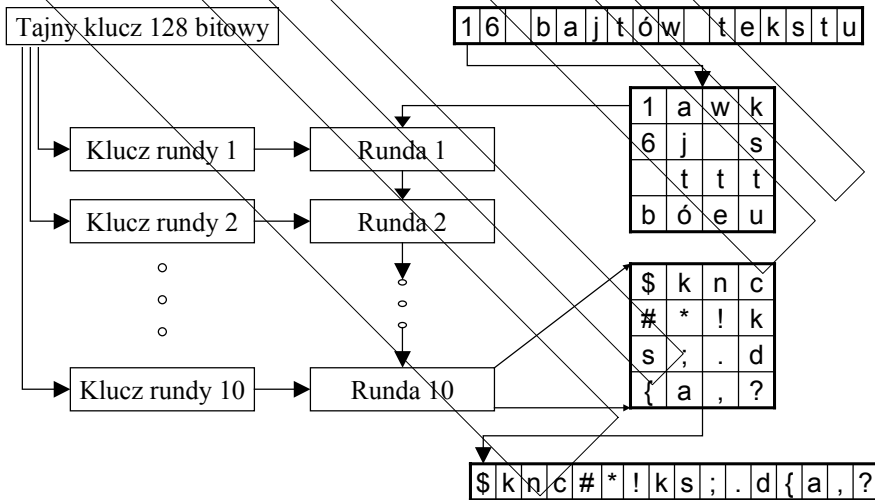
Wymagania postawione algorytmowi dla standardu AES

- ⇒ AES musi być algorytmem symetrycznym
- ⇒ Przetwarzać 128 bitowe bloki informacji
- ⇒ Pracować z kluczami 128, 192, 256 bitowymi
- ⇒ Odporny na znane metody kryptoanalityczne
- ⇒ Programowa i sprzętowa łatwość implementacji
- ⇒ Odporny na ataki metodą czasowa i poboru mocy (w przypadku kart chipowych)
- ⇒ Powinien być szybki zarówno w implementacjach programowych oraz sprzętowych
- ⇒ Małe potrzeby jeśli chodzi o zasoby systemowe
- ⇒ Wolny od opłat patentowych

Specyfikacja algorytmu AES

- Algorytm AES może pracować z kluczami o różnej długości tj.: 128, 192 i 256 bitów
- Przetwarza informację binarną w blokach o długości 128 bitów.
- Algorytm AES jest szybszy od 3DES około 4 razy. Przy programowej aplikacji AES osiąga prędkość szyfrowania 50 Mbps (dla klucza 256), podczas gdy 3DES 14 Mbps

Opis algorytmu AES dla klucza i danych o dł. 128-bitów



© Robert Borowiec

Kryptografia, Wykład VII
Strona 25/42

Właściwości algorytmu AES

- Jest odporny na znane metody kryptoanalityczne
- Jest to algorytm symetryczny. Do deszyfrowania trzeba jednak używać innego algorytmu i innych tabel

© Robert Borowiec

Kryptografia, Wykład VII
Strona 26/42

ALGORYTM IDEA

- W 1990 roku Algorytm Xuejia Lai i James Massey zaproponowali nowy algorytm szyfrowania -PES (*ang. Proposed Encryption Standard*).
- Pod aktualną nazwą algorytm IDEA zaistniał 1992r po wzmocnieniu go przeciw kryptoanalizie różnicowej.
- Obecnie jest to najlepszy algorytm dostępny publicznie (do zastosowań niekomercyjnych jest wolny od opłat).
- Stosowany jest między innymi w PGP (*ang. Pretty Good Privacy*)

ALGORYTM IDEA

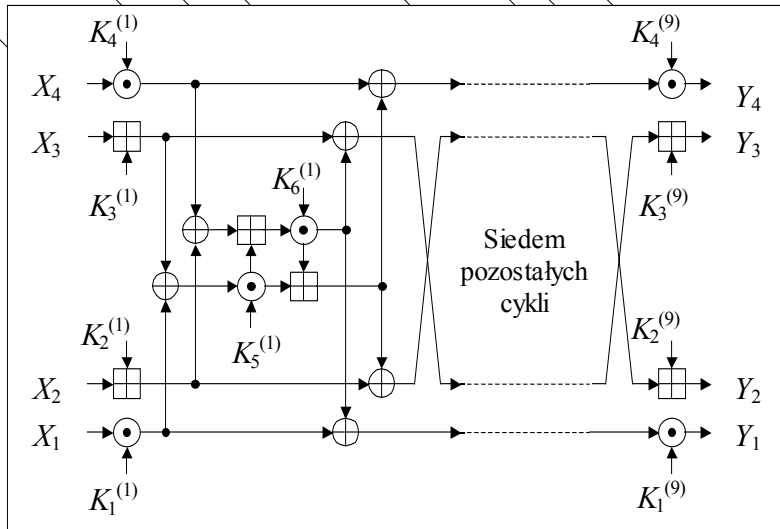
Algorytm przetwarza 64 bitowe bloki informacji i pracuje z kluczem 128 bitowym. Bazuje na :

- ⇒ mieszaniu
- ⇒ rozpraszaniu

W tym celu stosowane są operacje:

- ⇒ poelementowe dodawanie modulo 2
- ⇒ Dodawanie modulo 2^{16} (dodawanie z pominięciem przepelnienia)
- ⇒ Mnożenie modulo $2^{16}+1$ (mnożenie z pominięciem przepelnienia)

Schemat algorytmu IDEA



© Robert Borowiec

Kryptografia, Wykład VII
Strona 29/42

Kryptoanaliza algorytmu IDEA

- Algorytm IDEA jest odporny na analizę różnicową
- Atak brutalny wymaga sprawdzenia 2^{128} kluczy
- Maszyna złożona z miliarda układów scalonych, z który każdy testowałby miliard kluczy na sekundę, złamała by szyfrogram w ciągu 2^{43} lat, czyli w czasie dłuższym niż czas istnienia wszechświata

© Robert Borowiec

Kryptografia, Wykład VII
Strona 30/42

Tryby pracy szyfrów blokowych

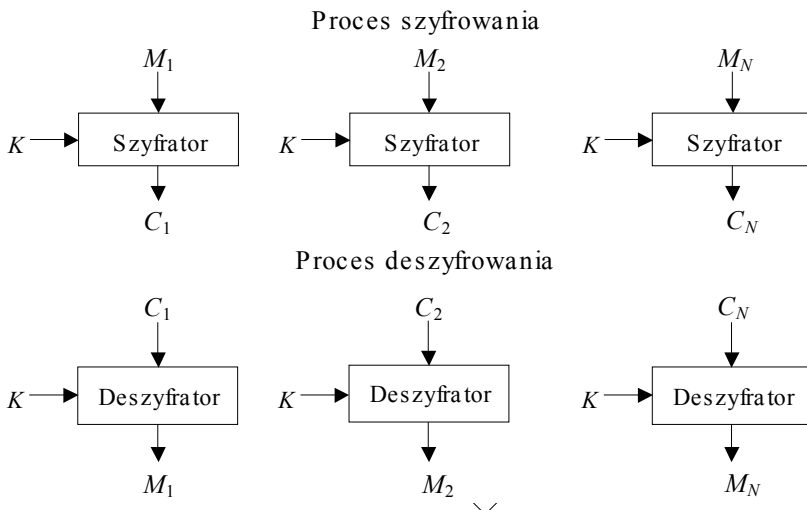
ECB -Electronic CodeBook -
elektroniczna książka kodowa

CBC -Cipher Block Chaining - wiązanie
bloków szyfrogramu

CFB -Cipher FeedBack - sprzężenie
zwrotne szyfrogramu

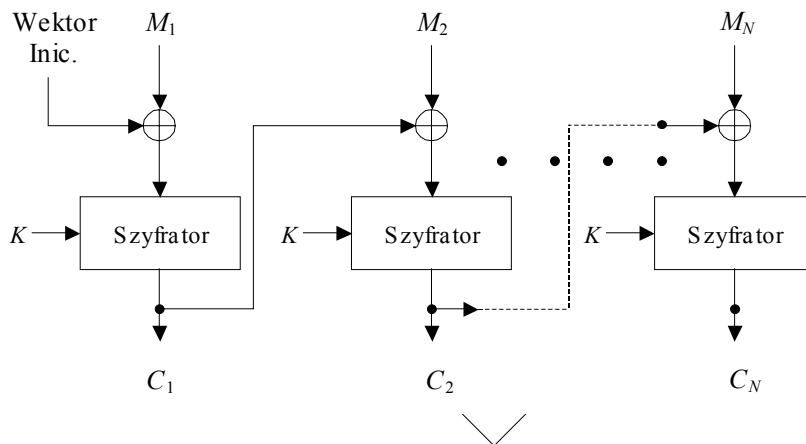
OFB -Output Feedback - wyjściowe
sprzężenie zwrotne

Elektroniczna książka kodowa (ECB)



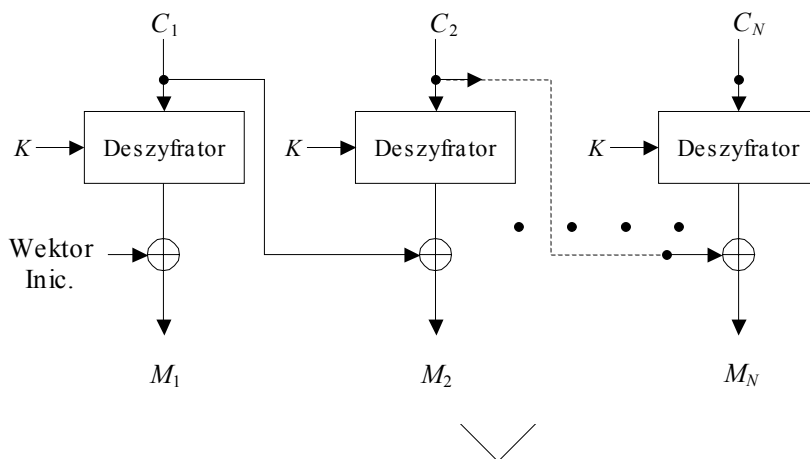
Wiązanie bloków szyfrogramu (CBC)

Proces szyfrowania



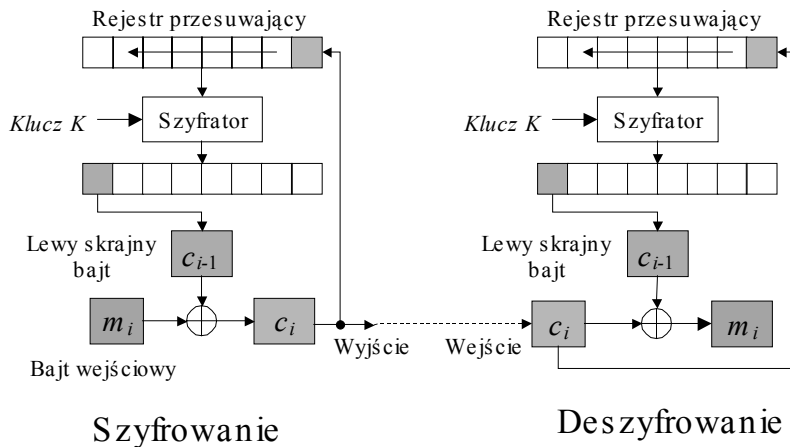
Wiązanie bloków szyfrogramu (CBC)

Proces deszyfrowania



Sprężenie zwrotne szyfrogramu

Cipher FeedBack

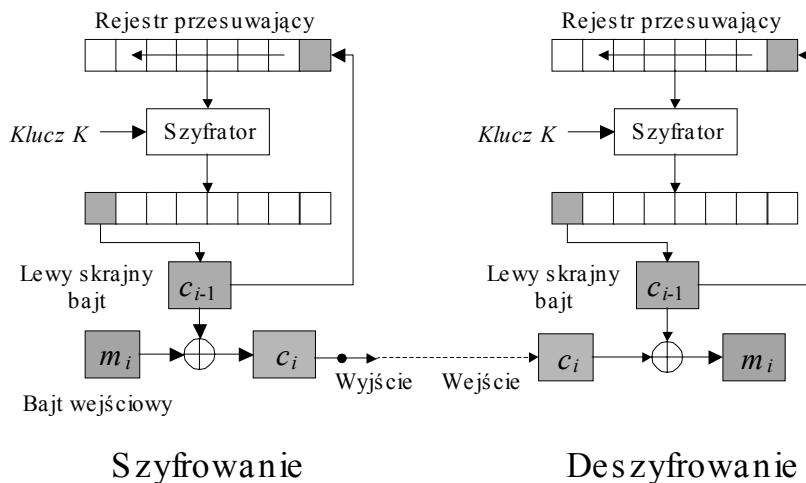


© Robert Borowiec

Kryptografia, Wykład VII
Strona 35/42

Wyściowe sprężenie zwrotne

Output FeedBack

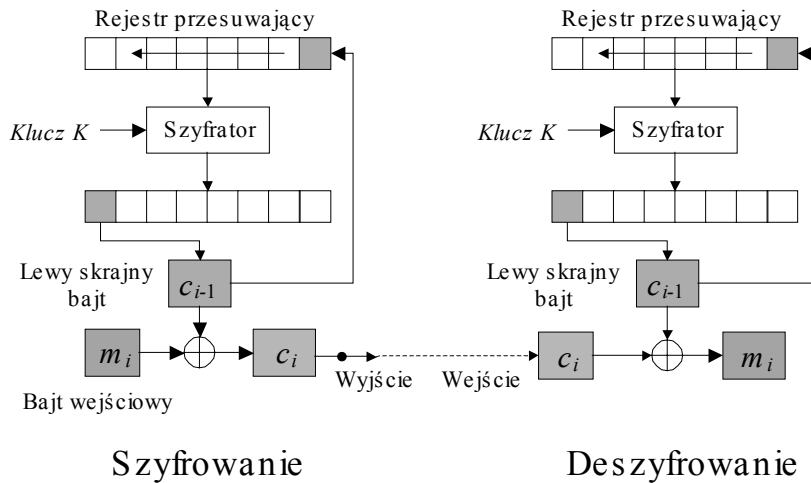


© Robert Borowiec

Kryptografia, Wykład VII
Strona 36/42

Wyjściowe sprzężenie zwrotne

Output FeedBack



© Robert Borowiec

Kryptografia, Wykład VII
Strona 37/42

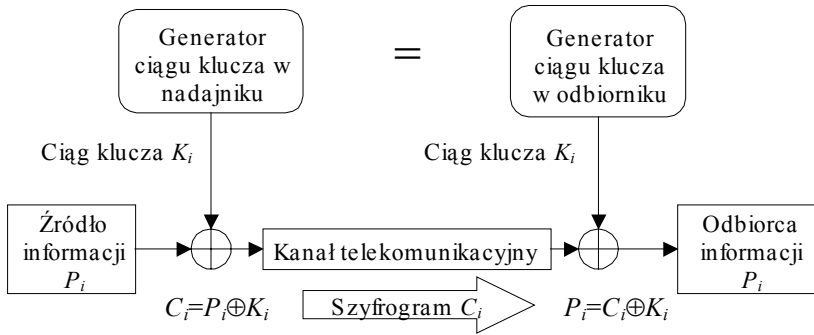
Szyfry strumieniowe

- Szyfry strumieniowe przekształcają tekst jawny bit po bicie.
- Najprostsza implementacja polega na sumowaniu XOR bitów informacji jawnej z bitami klucza.
- Deszyfrowanie odbywa się w identyczny sposób.
- Szyfry strumieniowe stosuje się w kanałach telekomunikacyjnych o dużej przepustowości

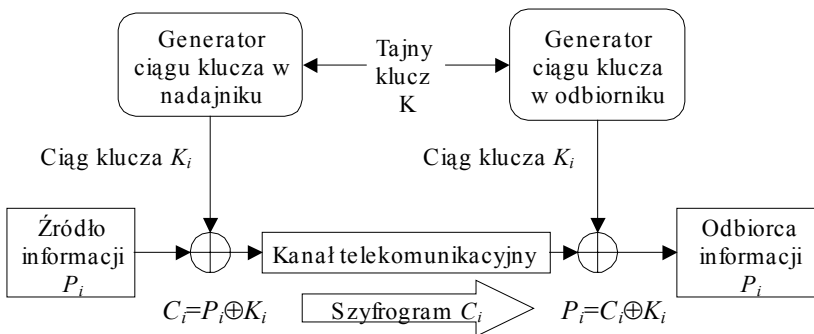
© Robert Borowiec

Kryptografia, Wykład VII
Strona 38/42

Szyfry strumieniowe



Szyfry strumieniowe



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

KONIEC

Dziękuję za uwagę