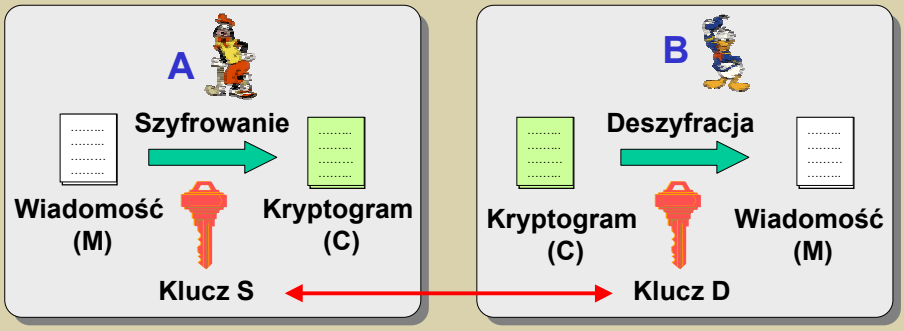
Elementy kryptografii

Szyfrowanie danych przy użyciu kluczy symetrycznych część II

Szyfry z kluczem symetrycznym



Szyfr z kluczem symetrycznym

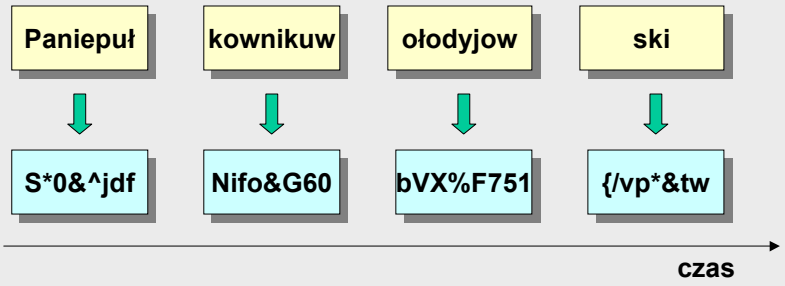
⇩

Klucz szyfrowania (S) i klucz deszyfracji (D) są takie same

Szyfry blokowe

- Szyfr strumieniowy - szyfrowanie kolejne bity
- Szyfr blokowy - jednoczesne szyfrowanie grupy bitów (powszechnie - bloki 64 bitowe)

Przykład: „Panie pułkowniku Wołodyjowski”



Współczesne szyfry z kluczem symetrycznym

Technika szyfrowania

- Kombinacje przestawień i podstawień
- Szyfry blokowe

Bezpieczeństwo szyfrów

- Atak tylko metodą prób i błędów
- Złożoność - wykładnicza funkcja długości klucza

Powszechnie stosowane szyfry

- DES (56b) - 3DES (2,3 x 56b) - AES(128b ...)
- IDEA(128b)
- Lucifer, Blowfish ...

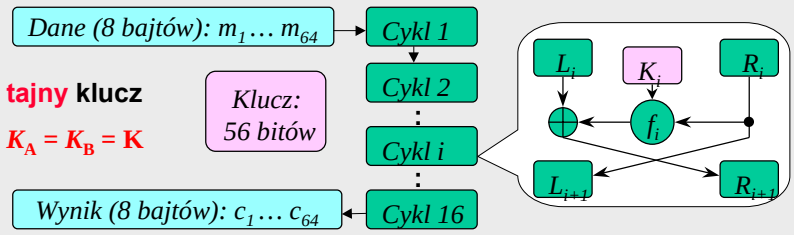
Bezpieczeństwo szyfrów

Czasy sprawdzenia wszystkich kluczy w funkcji długości klucza

Długość klucza	Procesor 1GHz (10^6 kluczy/s)	Milion proc. 1GHz (10^{12} kluczy/s)
56	**1000 lat**	**10 godzin**
64	**2.9×10^5 lat**	**107 dni**
96	**1.3×10^{18} lat**	**1.3×10^{12} lat**
128	**5.4×10^{24} lat**	**5.4×10^{18} lat**

Przegląd szyfrów

Algorytm DES (1976)



f_i ⇒ **S - box** (Podstawienia) **P - box** (Przestawienia)

Algorytm DES

Podstawienia

Indeks kolumn $x_4 x_3 x_2 x_1$

Struktura tablicy podstawień (S-box)

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
2	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

Dane:

$\mathbf{x} = x_5 x_4 x_3 x_2 x_1 x_0$

$x_5 x_0$ *Indeks wierszy*

Wynik: $y_3 y_2 y_1 y_0$

Przykład

$x_5 x_4 x_3 x_2 x_1 x_0 = 011011$ → *Wiersz -* $(01)_2 = 1$ *Kolumna -* $(1101)_2 = \mathbf{13}$

$\mathbf{y} = f(1,13) = 5 = 0101$

Algorytm DES

Przestawienia

Struktura tablicy przestawień (P-box)

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

Dane

$\mathbf{x} = x_5 x_4 x_3 x_2 x_1 x_0$

$\mathbf{P} = i_5 i_4 i_3 i_2 i_1 i_0$

Wynik

$\mathbf{y} = y_5 y_4 y_3 y_2 y_1 y_0 =$

$x(i_5) x(i_4) x(i_3) x(i_2) x(i_1) x(i_0)$

Przykład

$\mathbf{P} = i_5 i_4 i_3 i_2 i_1 i_0 = 531240$

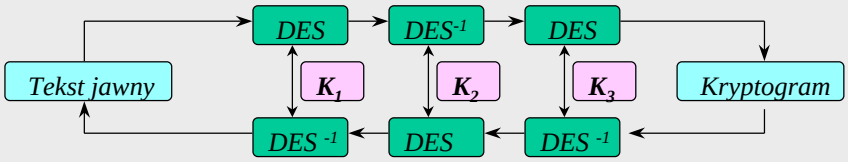
$\mathbf{x} = x_5 x_4 x_3 x_2 x_1 x_0 = 010101$

→ $\mathbf{y} = 111000$

Przegląd szyfrów

Złamanie DES (lata 90-te "kryptoanaliza różnicowa"- moc algorytmu ok. 2^{38})

3DES



3DES - moc szyfru zwiększona do ok. 2^{70} (wiek wszechświata - 2^{68} s)

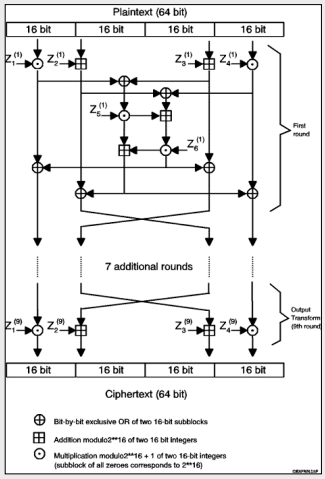
Inne właściwości

- Szybkość szyfrowania / deszyfracji
  - Hardware - 100 Mb/s, software (P1.4) - 10Mb/s
- 2 złe i 4 słabe klucze

Przegląd szyfrów

Algorytm IDEA

- Szyfr blokowy (8 bajtów)
- Klucz 128-bitowy
- Taki sam algorytm szyfrowania i deszyfracji
- Szybkość - podobna jak dla DES
- Chroniony patentem

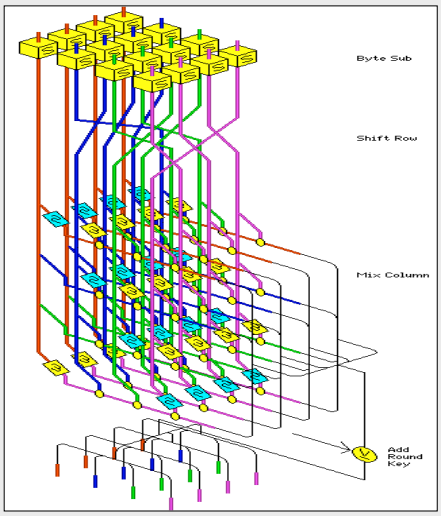


http://www.anujseth.com/crypto/blockciphers/idea.html

Przegląd szyfrów

Algorytm AES
('Rijnadel')

- Szyfr blokowy (16 bajtów)
- Klucz - 128, 192, 256 bitów
- Zmienna liczba rund (9, 11 lub13)
- Prostsza struktura niż w DES
- Taki sam algorytm szyfrowania i deszyfracji
- Szybkość - większa niż dla DES



http://home.ecn.ab.ca/~jsavard/crypto/co040801.htm

Szyfry blokowe - technika CBC

Podstawowy schemat szyfrowania ...

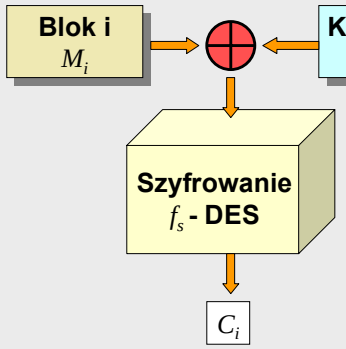
Wiadomość 1	Depozyt:	$10000,0	Nr konta	56-2345-	85693-4
Kryptogram 1	J8ydoi3-	Hdy&546s	Bdgt^&gd	#40vbshe	J8ydoi3
Wiadomość 2	Depozyt::	$1000,00	Nr konta	26-2311-	999947-4
Kryptogram 2	J8ydoi3-	dgeTui)i	Bdgt^&gd	89dophkj	.ladjrpo
Spreparowany kryptogram	J8ydoi3-	Hdy&546s	Bdgt^&gd	89dophkj	.ladjrpo

... pozwala na manipulację wiadomością bez konieczności poznawania klucza

Szyfry blokowe - technika CBC

Wiązanie bloków

Obrona przed manipulacją szyfrogramem



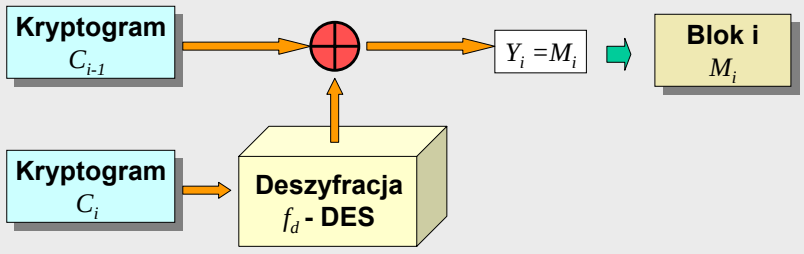
$$C_0 = f_s(M_0)$$

$$C_i = f_s(M_i \oplus C_{i-1})$$

Bezpieczeństwo systemów informatycznych

Szyfry blokowe - technika CBC

Wiązanie bloków



$$Y_i = f_d(C_i) \oplus C_{i-1} = f_d(f_e(M_i \oplus C_{i-1})) \oplus C_{i-1} = M_i \oplus C_{i-1} \oplus C_{i-1} = M_i$$

Krzysztof Ślot © 2002

Kryptografia a rządy

- **Ograniczenia eksportowe**
  - **Moc szyfru ustalona w sposób sugerujący możliwość przełamania**
- **Ingerencje w tajność korespondencji**
  - **Celowe przemycanie mechanizmów ułatwiających łamanie w sprzedawanych systemach (DES, Francja i kontrakt na szybką kolej dla Korei Południowej)**
  - **NSA - dostęp do danych bankowych, podsłuch i deszyfracja telefonii komórkowej**
  - **Eszelon (Eshelon)**

Bezpieczeństwo systemów informatycznych

Kryptografia a rządy

Eshelon - Globalny system podsłuchu i analizy informacji

- Zaprojektowany i nadzorowany przez NSA
  Nasłuch - satelity, anteny naziemne, monitorowanie ruchu w Internecie, podsłuch (np. odkryty w 1982) podmorskich kabli (włączając światłowodowe)

Stacja nasłuchowa w Menwith Hill Station, UK ($52^0$52”N,$3^0$3”W) - 2 miliony przechwyceń na godzinę

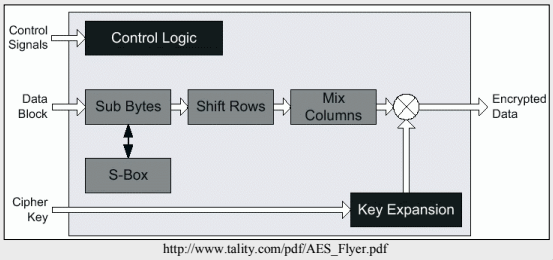
- Główne cele - niemilitarne (szpiegostwo przemysłowe, bezpieczeństwo wewnętrzne)
  Parlament Europejski wystosował w ostatnich dwóch latach kilka not protestacyjnych

Krzysztof Ślot © 2002

Dodatek - sprzętowe realizacje AES (2002)

Cadence Design Foundry

- Pełna implementacja standardu (dane 128b, klucze 128, 192, 256 b)
- Tryby pracy ECB, CBC
- 960 Mb / s przy 83 MHz



http://www.tality.com/pdf/AES_Flyer.pdf

Ocean Logic

- Pełna implementacja standardu (dane 128b, klucze 128, 192, 256 b)

Core	Datapath Width	Approx. Area	Throughput bits/cycle	Throughput at 200 MHz
Encryption only core without key expander	32	4 Kgates	~2.9	~580 Mbit/s
	128	16 Kgates	~11.6	~2.32 Gbit/s
Encryption/Decryption core without key expander	32	6 Kgates	~2.9	~580 Mbit/s
	128	24 Kgates	~11.6	~2.32 Gbit/s
Key expander core	32	8 Kgates	~2.9	~580 Mbit/s
	128	32 Kgates	~11.6	~2.32 Gbit/s