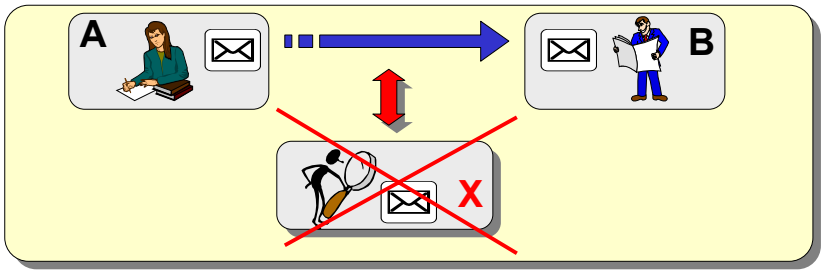
Elementy kryptografii

Szyfrowanie danych przy użyciu kluczy symetrycznych

Szyfrowanie danych = ukrycie treści



Jak utajniać dane?

Albert: „Jak wezmę to pomarańczowe, to znaczy ‘padnij’”

[Seksmisja]

Wady - za dużo współdzielonej informacji, brak reguły

Szyfrowanie danych

“doohd ldfxd hwx”

[Juliusz Cezar]

Szyfr Cezara

‘Nowoczesny’ szyfr - precyzyjny algorytm kodowania + tajna informacja potrzebna do deszyfracji

Zasada kodowania

$c_i = (m_i + k) \bmod n$

k - klucz

c_i- litera kodu, m_i - litera wiadomości, n - liczba znaków alfabetu

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	w	x	y	z

k = 3

d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	w	x	y	z	a	b	c

gladiator → **j o d g l dx r u**

Szyfr Cezara

doohd ldfxd hwx —($k=3$, A→ D, B→ E ...)→ **allea iacta est**

[Juliusz Cezar]

Szyfr Cezara - szyfr podstawieniowy

Jak złamać szyfr Cezara ?
(czyli odczytać zaszyfrowaną wiadomość)

Bezpieczeństwa szyfru Cezara chroni przede wszystkim algorytm szyfrowania

Znając algorytm łatwo odnaleźć k dające sensowną treść wiadomości

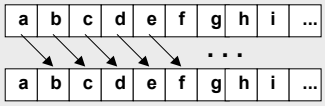
?: ntktxrfzdpf

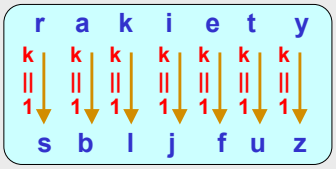
Ewolucja szyfrów podstawieniowych

Zmiana zasady kodowania liter - zmienna wartość przesunięcia

Stała wartość przesunięcia (szyfr Cezara)

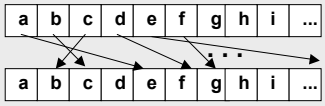
k = 1

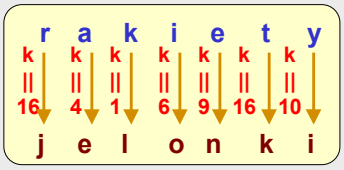




Zmienna wartość przesunięcia

k = var



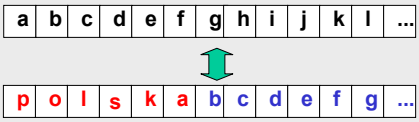


Ewolucja szyfrów podstawieniowych

Jak zapamiętać kody przypisane kolejnym znakom ?

Użyć sekretnego słowa - klucza, np.:

'polska'



Zwiększenie długości klucza - większe zróżnicowanie zasad zastępowania liter

Jak złamać szyfr podstawieniowy z kluczem ?

➡ **Metoda prób i błędów - analiza wszystkich możliwych kluczy**

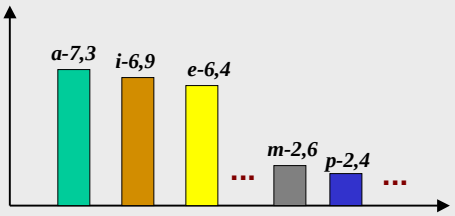
3 literowe = 3! = 6 ; 4 literowe = 4! = 24 ; 5 literowe = 5! = 120 ;

... 14 literowe = 14! = 87 178 291 200 ➡ dla długich kluczy - zadanie nierealne

Szyfry podstawieniowe, c.d.

Bezpieczna metoda szyfrowania ? ☹

Charakterystyczna cecha każdego języka - częstości występowania znaków i grup znaków



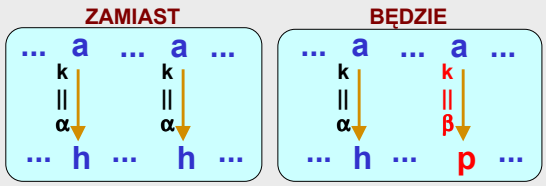
Analiza częstości występowania znaków pozwala na łatwe łamanie szyfrów, w których relacja znak tekstu jawnego - znak kodu jest jednoznacznie określona

Szyfry podstawieniowe monoalfabetyczne nie zapewniają skutecznej ochrony danych

Szyfry wieloalfabetyczne

Cel: ukryć częstość występowania znaków

Zasada kodowania nie jest stała



Zasada szyfrowania

Klucz: N a j l e p s z e k a s z t a n y są na placu Pigalle

Przesunięcie (k): 14 10 5 0 12 .....

Tekst jawny: Przejmuję władzę jutro po kolacji → Frj...

P → f (k=14) r → r (k=0) z → j (k=10) .....

Szyfry wieloalfabetyczne

Właściwości metody

Metoda maskuje częstości występowania liter i zapewnia teoretyczną nieprzełamywalność szyfru jeżeli

- **klucz jest nie krótszy od wiadomości**
- **kluczem jest ciąg liczb losowych**

W przeciwnym razie klucz staje się 'okresowy', przy czym długość okresu szyfru można oszacować (metoda Kasiskiego)

a wtedy, im krótszy klucz, tym łatwiej złamać szyfr

Szyfry wieloalfabetyczne

Wniosek: trzeba wydłużać długość klucza

Używanie długiego klucza wymaga wsparcia maszyny

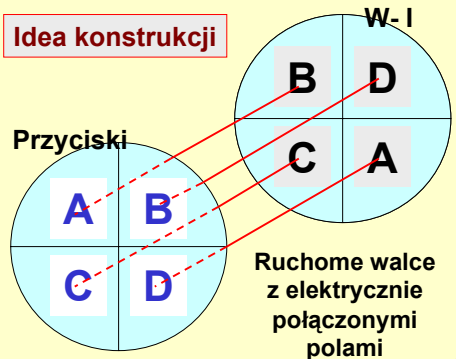
ENIGMA

Pierwsza faza 'wojny' z ENIGMĄ
1933-39 - złamanie szyfru
M.Rejewski, J.Różycki, H.Zygalski

1934 - zapowiedź 'nocy długich noży'
...
1938 - aneksja Czech

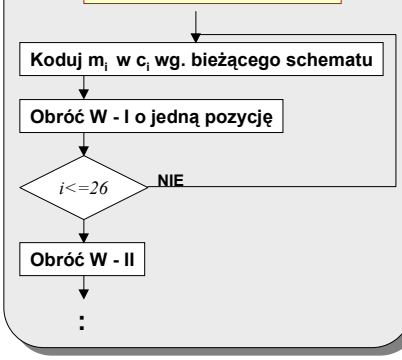
ENIGMA

Idea konstrukcji



Ruchome walce z elektrycznie połączonymi polami

Algorytm działania



Przykład **Tekst jawny - BABA** **Kryptogram - ABBA**

1 B → A 2 obrót 3 A → B 5 B → B 7 A → A

ENIGMA

Podstawowe właściwości

Okres powtarzania klucza - 26^n gdzie n - liczba walców

→ Enigma ‘trójtarczowa’ (do wybuchu wojny cała armia, po - wojska lądowe)

‘Długość’ klucza: $26^3 = 17576$

→ Enigma ‘pięciotarczowa’ (od wybuchu wojny marynarka i lotnictwo)

‘Długość’ klucza: $26^5 = 11\,881\,376$

ENIGMA miała pewną wadę, która wydatnie pomogła w złamaniu szyfru

Współczesna kryptografia

Kryptografia ery komputera

Łamanie szyfrów - podstawowy czynnik stymulujący powstanie komputerów

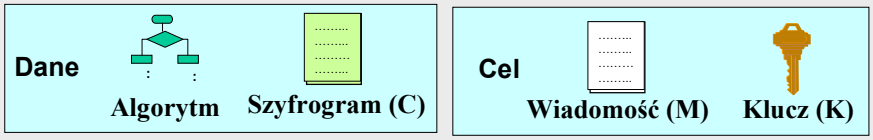
1940 - A. Turing, 1943 - K. Zeusse (Niemcy) maszyny do "łamania" szyfrów
ENIAC (1943) - podstawowe zadanie - krytpografia

Założenie 1 współczesnej kryptografii

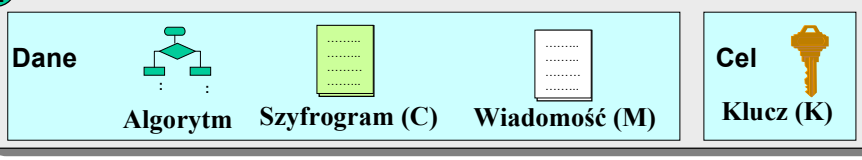
Algorytm szyfrowania jest niemożliwy do utajnienia

Rodzaje "ataków" kryptograficznych

1 Atak z tekstem zaszyfrowanym



2 Atak z tekstem jawnym / z tekstem spreparowanym



Założenie 2 współczesnej kryptografii

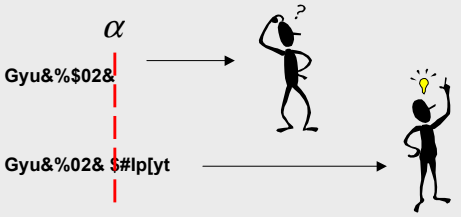
Najbardziej prawdopodobny atak ze spreparowanym tekstem jawnym

Bezpieczeństwo szyfru zależy całkowicie od klucza
Odgadnięcie klucza musi być nierealne

Ilościowe charakterystyki szyfrów

Entropia Miara przypadkowości znaków w tekście

Długość krytyczna szyfru α



Poufność doskonała: $\alpha \rightarrow \infty$ (szyfr z kluczem jednokrotnym)

Szyfry przestawieniowe (anagramy)

Idea szyfrowania - zamiana miejscami znaków tekstu

Rodzaje szyfrów przestawieniowych

- **Szyfry bez kluczy**
  Tajność wiadomości zapewnia wyłącznie algorytm szyfrowania
  Przykłady - szyfr 'parkanowy'

- **Szyfry z kluczem**
  Tajność wiadomości jest chroniona przez sekretną informację
  Przykłady - Playfair (I wojna światowa)

Szyfry przestawieniowe

Szyfr 'parkanowy'

Zasada tworzenia kryptogramu

Tekst jawny: Główną gonitwę wygra Tornado

➡ **Co drugi znak przepisujemy do drugiej linii,**

Góngntęyrtrao
łwąoiwwgaond

➡ **Łączymy utworzone w ten sposób ciągi**

Kryptogram: Góngntęyrtraołwąoiwwgaond

Szyfry przestawieniowe

Publiczne deponowanie sekretu

Problem - jak opublikować sekret, a jednocześnie go nie wyjawić?

Metoda - anagramy grupujące alfabetycznie litery tekstu

Tajemnica
Jutro spadnie deszcz

➡

Kryptogram
acddeeijnoprsstuzz

Właściwości szyfrów przestawieniowych

➡ **analiza częstości nie pomaga rozszyfrować wiadomości**

➡ **są tak samo trudne do złamania jak szyfry podstawieniowe wieloalfabetyczne**

Podsumowanie

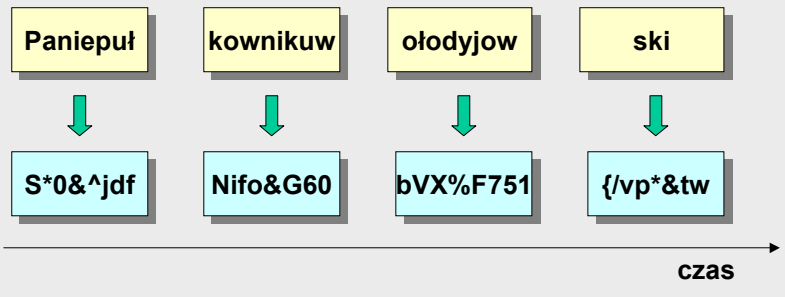
- **Rodzaje technik szyfrowania**
  - Podstawienia
  - Przestawienia
- **Założenia współczesnej kryptografii**
  - Jawność algorytmu szyfrowania
  - Jawność pary: tekst - szyfrogram
- **Najważniejszy element szyfru**
  - Klucz

Klucz do szyfrowania i do deszyfracji taki sam → **Klucz symetryczny**

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 ...

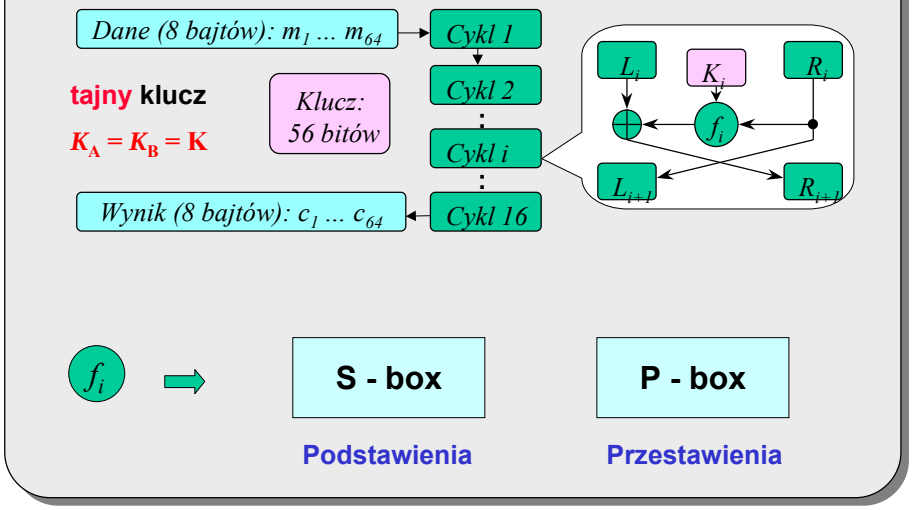
Bezpieczeństwo szyfrów

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

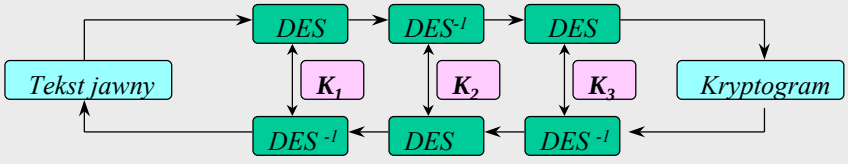
Algorytm DES (1976)



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)

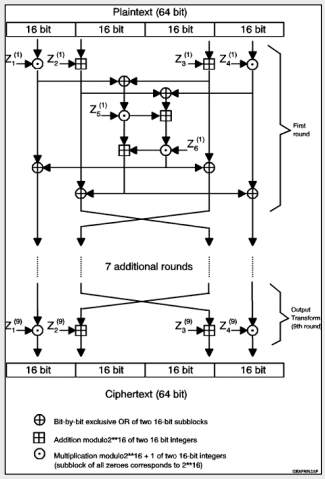
Inne właściwości

- **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

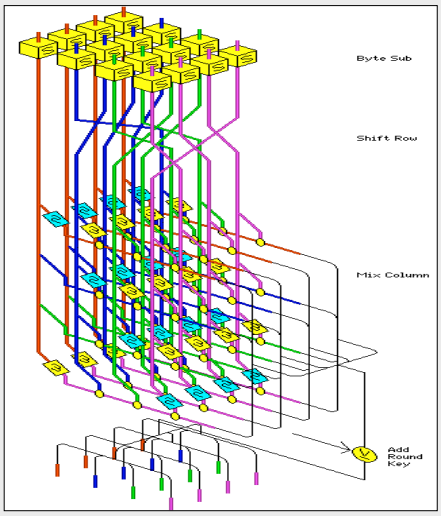


http://www.anujseth.com/crypto/blockciphers/idea.html

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 ...

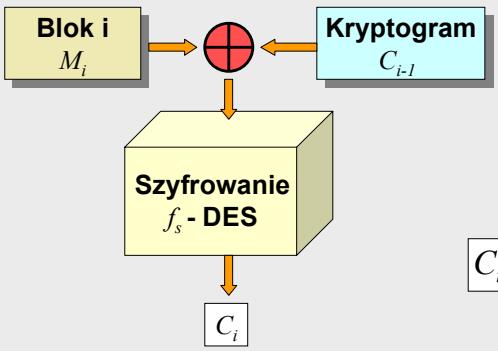
Wiadomość 1	Depozyt:	$10000,0	Nr konta	56-2345-	85693-4
Kryptogram 1	J8ydoi3-	Hdy&546s	Bdgt^&gd	#40vbshe	J8ydoi3
Wiadomość 2	Depozyt::	$1000,00	Nr konta	26-2311-	999947-4
Kryptogram 2	J8ydoi3-	dgeTui)i	Bdgt^&gd	89dophkj	.ladjrpo
Spreparowany kryptogram	J8ydoi3-	Hdy&546s	Bdgt^&gd	89dophkj	.ladjrpo

... pozwala na manipulację wiadomością bez konieczności poznawania klucza

Szyfry blokowe - technika CBC

Wiązanie bloków

Obrona przed manipulacją szyfrogramem

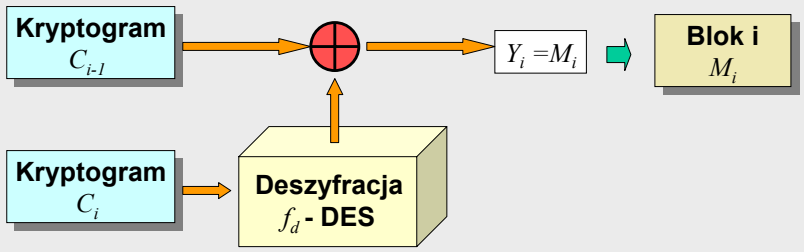


$$C_0 = f_s(M_0)$$

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

Szyfry blokowe - technika CBC

Wiązanie bloków



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

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)

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

LPMJFD