Szyfry symetryczne i asymetryczne

dr inż. Krzysztof Cabaj

Plan wykładu

- Pojęcia podstawowe
- Trochę historii
- Szyfry strumieniowe i blokowe
- Szyfry symetryczne i asymetryczne
- Tryby działania szyfrów blokowych

Podstawowe pojęcia

- Kryptografia – nauka i sztuka o projektowaniu szyfrów
- Kryptoanaliza – sztuka i nauka łamania szyfrów
- Kryptologia = kryptografia + kryptoanaliza

- Steganografia – sztuka ukrywania informacji

Podstawowe pojęcia

- Tekst jawny – dane przed zaszyfrowaniem (niekoniecznie musi być to tekst !!!)
- Szyfrogram – zaszyfrowane dane

- Klucz – modyfikuje działania algorytmu, dzisiejsze założenie co do szyfrów: algorytm jest jawny a bezpieczeństwo tkwi w tajnym kluczu

Podstawowe pojęcia

- Szyfrowanie a kodowanie
- Celem szyfrowania jest zapewnienie poufności
- Kodowanie to sposób reprezentacji pewnych danych w dobrze zdefiniowany sposób, przykładowo
  - kod ASCII
  - kod Morse'a
  - Kod Breille'a
  - Kod Manchester

Szyfry wykorzystujące przestawienie

- W celu zaszyfrowanie informacji (tekstu), przestawiamy zgodnie ze znanym algorytmem kolejność znaków znajdujących się w szyfrowanym tekście uzyskując szyfrogram

Scytale

- Przykład antyczny – scytale (lub skytale), drewniany „walec” na który nawijano pasek papieru/skóry i pisano tekst

Rysunek. Wikipedia

- Jeśli owinięto taki pasek wokół pasa, literami do wewnątrz możemy mówić także o steganografii

Szyfr Playfair (-a)

- Kluczem jest kwadratowa macierz 5x5 z wypisanymi wszystkimi literami alfabetu (litery ‚i' oraz ‚j' są w jednym polu)

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

- Szyfrowaniu podlegają dwie litery tekstu jawnego, jak są identyczne wstawia się literę x

Szyfr Playfair (-a)

- Algorytm szyfrowania
  - Jak obie litery znajdują się w tym samym wierszu zastępujemy je kolejnymi literami (z przeniesieniem)
  - Jak obie litery znajdują się w tej samej kolumnie, zastępujemy literami leżącymi bezpośrednio pod (z przeniesieniem)
  - W innym przypadku bierzemy litery, z „pozostałych rogów” wyznaczonego prostokąta

Szyfr Playfair (-a)

- Przykłady

MI -> NK

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

GE -> OG

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

ME -> DG

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

Szyfry wykorzystujące podstawienie

- W celu zaszyfrowanie zastępujemy literę w tekście jawnym inną literą i w ten sposób uzyskujemy tekst szyfrogramu

Szyfr Cezara

- Przesuwa każdą literę o 3

  A -> D

  B -> E

  . . .

- Matematycznie można zapisać

  C=(M+K) mod 26

- Szyfr monoalfabetyczny – używamy jednego alfabetu szyfrującego
- W szyfrze Cezara proste przesunięcie liter ale można stosować dowolną permutację liter w alfabecie szyfrującym

Szyfr polialfabetyczny

- Używamy kilku alfabetów szyfrowych (permutacji), pierwszą literę szyfrujemy za pomocą pierwszego, drugą za pomocą drugiego itd. …, po ostatnim używanym alfabecie wykorzystujemy kolejny raz pierwszy, itd. …
- Jest to szyfr polialfabetyczny – mamy wiele alfabetów szyfrujących
- Przed wymianą informacji należy uzgodnić liczbę i permutacje w alfabetach szyfrujących
- Vigenere-a zaproponował metodę tworzenia szyfru polialfabetycznego opartego jedynie o klucz (słowo), oraz ułatwienie szyfrowania w oparciu o tak zwane tablice Vigenere-a

Szyfr Vigenere-a – tablica Vigenere-a

Jawny	A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
1	B C D E F G H I J K L M N O P Q R S T U V W X Y Z A
2	C D E F G H I J K L M N O P Q R S T U V W X Y Z A B
3	D E F G H I J K L M N O P Q R S T U V W X Y Z A B C
4	E F G H I J K L M N O P Q R S T U V W X Y Z A B C D
5	F G H I J K L M N O P Q R S T U V W X Y Z A B C D E
6	G H I J K L M N O P Q R S T U V W X Y Z A B C D E F
7	H I J K L M N O P Q R S T U V W X Y Z A B C D E F G
. . .	. . .
26	A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Szyfr Vigenere-a

Słowo kluczowe	K I N G K I N G K I N G . . .
Tekst jawny	A L A M A K O T A . . .
Tekst zaszyfrowany	K T N S K S B Z K

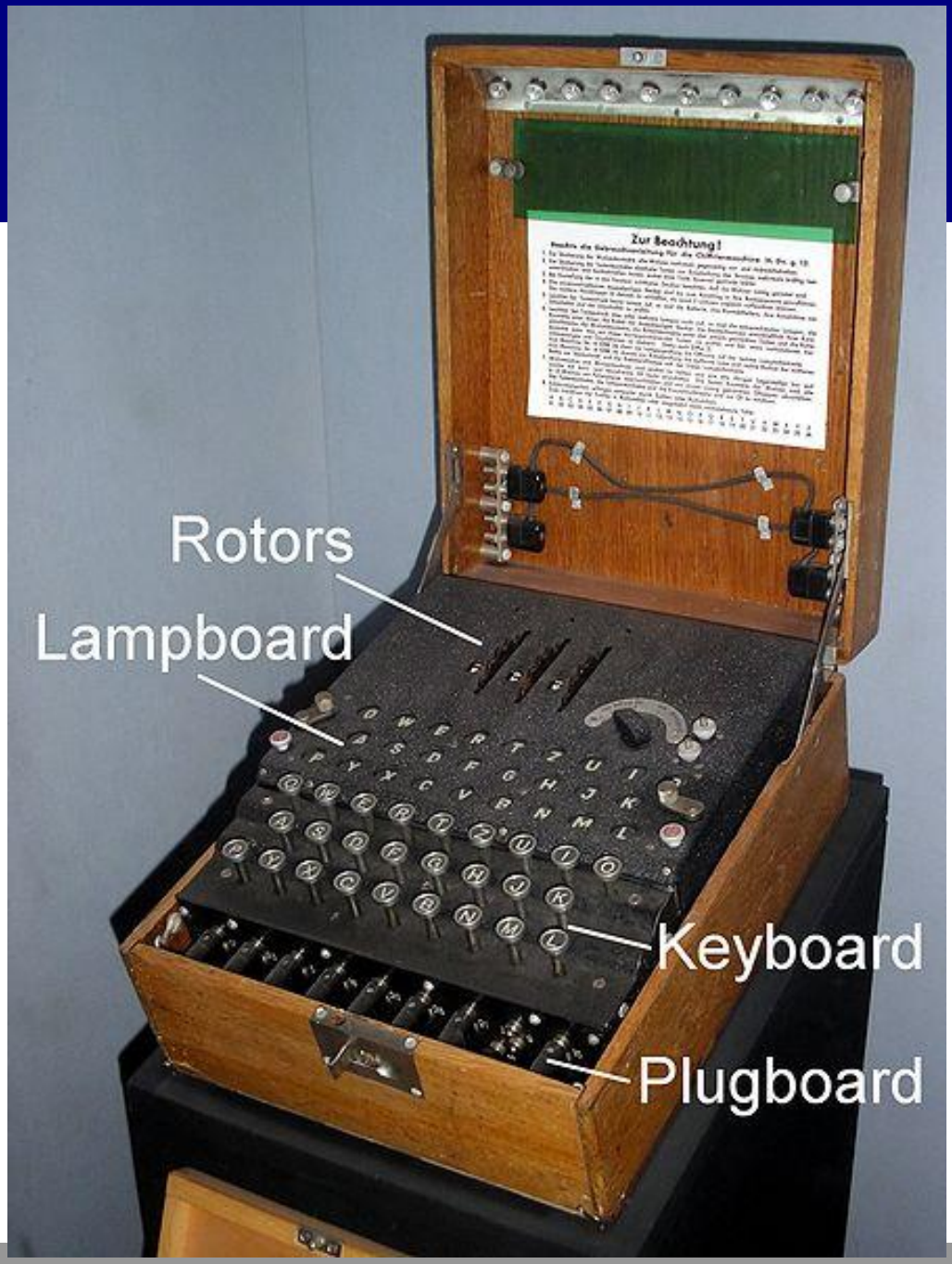
Szyfr Vernama

- Postępowanie analogiczne jak w szyfrze Vigenera, ale z jednorazowym kluczem o długości identycznej jak wiadomość
- Szyfr którego nie da się złamać (przy zapewnieniu warunku o niepowtarzalności klucza)

Maszyny rotorowe

- Tablice Vigenere-a ułatwiają szyfrowanie ale nadal są skomplikowane w szybkiej obsłudze
- Ułatwienie szyfrowania z wykorzystaniem „nowoczesnej” techniki – baterii i żaróweczek ;)
- Maszyna składa się z:
  - klawiatury
  - rotorów/bębenków – realizujących szyfr podstawieniowy/permutację
  - tablicy z lampkami – służy do odczytania
- Przykłady maszyn rotorowych
  - Enigma
  - Japońska maszyna/szyfr Purple

Enigma



Rysunek. Wikipedia

Enigma

- Siła Enigmy
  - 3 bębenki (w późniejszym etapie wybierane z większego zestawu)
  - Po każdej literze następuje przekręcenie ostatniego bębenka do kolejnej pozycji, po 26 zmianach przekręca się środkowy bębenek, po 26*26 zmianach przekręca się pierwszy bębenek – daje to klucz o długości 26^3 znaków (17,5 tysiąca)
  - Dodatkowo możliwość podmiany dwóch liter po wyjściu sygnału z bębenków

Podział szyfrów

- Szyfry blokowe i strumieniowe
- Szyfry symetryczne i asymetryczne

Szyfry strumieniowe

- Szyfrujemy nadchodzący znak, bajt, bit niezależnie

- Przykłady historyczne
  - Szyfr Cezara
  - Szyfr Vigenera
  - Szyfr Vernama
- Przykłady współczesne
  - RC4 wykorzystywany przez algorytm WEP, PPTP (a także opcjonalnie przez SSH i SSL)

Wersja współczesna (cyfrowa) szyfru podstawieniowego

- Jeśli działamy na danych cyfrowych można skorzystać z funkcji logicznej XOR (Exlusive OR)
- Tablica prawdy funkcji XOR

X	Y	X xor Y
0	0	0
0	1	1
1	0	1
1	1	0

- Szyfrowanie polega na dokonaniu operacji XOR na wiadomości i strumieniu klucza

Szyfr strumieniowy (współcześnie)

- Funkcja z kluczem generująca ciąg pseudolosowy
- Ciąg zostaję połączony z wiadomością do zaszyfrowania za pomocą funkcji XOR

- C = M xor K

- Oprócz używanego (aczkolwiek złamanego) RC4, jako szyfry strumieniowe można używać specjalne tryby szyfrów blokowych (więcej w dalszej części tego wykładu)

- Uwaga szyfry RC5 i RC6 są szyframi blokowymi !!!

Szyfry blokowy

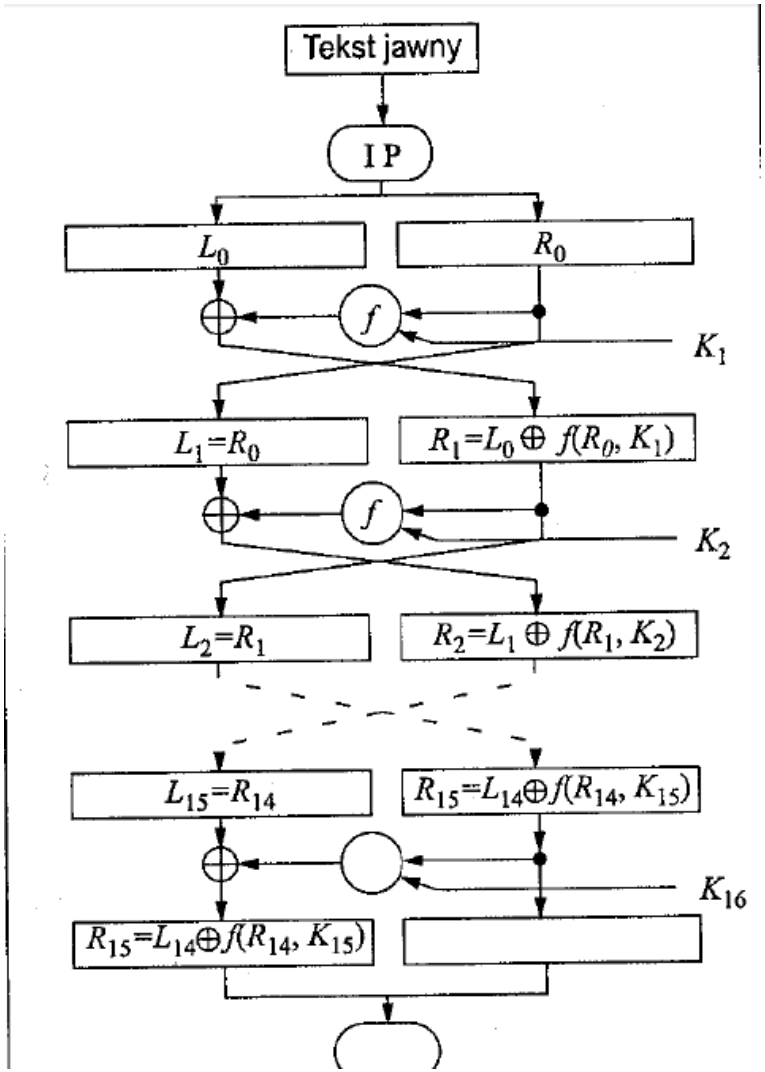
- Szyfrujemy za jednym razem większą porcję danych niż znak
- Pierwsze rozwiązania historyczne szyfrowały dwie litery na raz (była to obrona przed atakami częstościowymi) …
- … współczesne działają na blokach wielkości od 64 bitów do 128 bitów

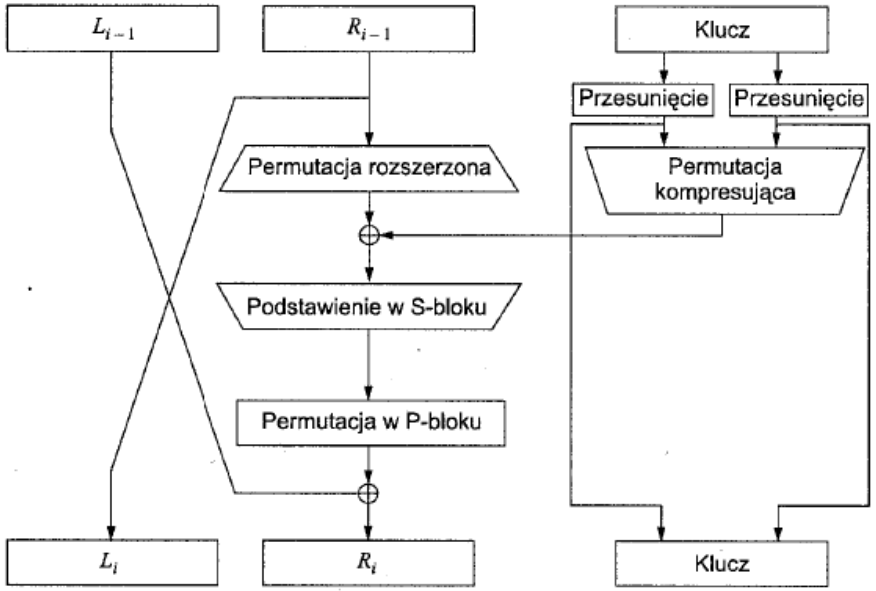
Szyfry blokowe

- Siła szyfrów blokowych polega na wielokrotnym zastosowaniu prostych operacji takich jak zmieszanie i rozproszenie

- Analogia do starych, historycznych metod jak podstawienie i przestawienie

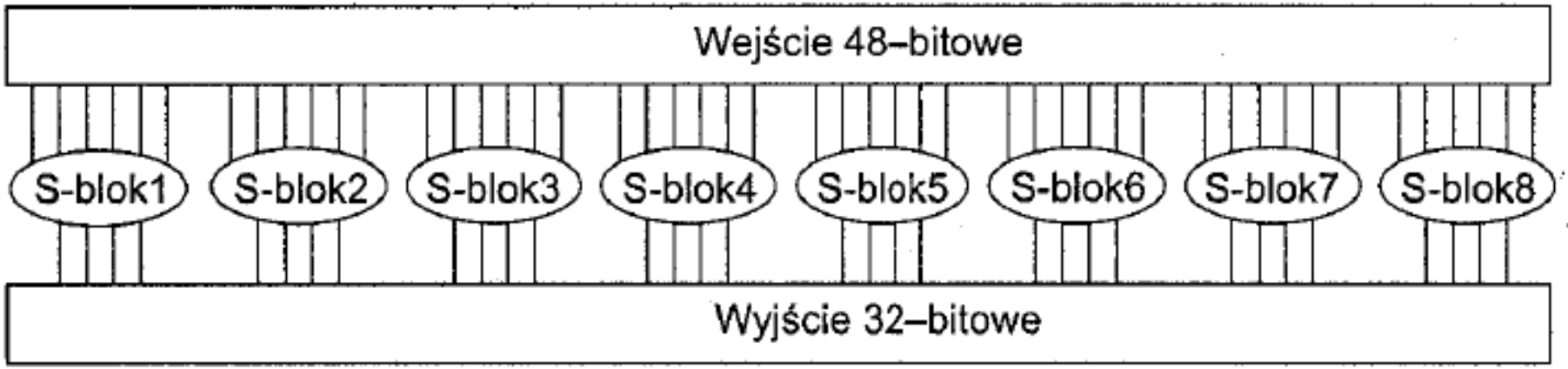
Szyfry blokowe, przykład DES





Rysunki. Bruce Schneier, Kryptografia dla praktyków

Szyfry blokowe, przykład DES



Rysunek. Bruce Schneier, Kryptografia dla praktyków

Szyfry blokowe

- Najpopularniejsze szyfry blokowe
  - DES (nie należy używać !!!)
  - 3DES
  - AES/Rijndael (preferowany)

Podział szyfrów: symetryczne i asymetryczne

- Szyfry symetryczne używają jednego klucza do szyfrowania i odszyfrowywania danych
  - Mówimy wtedy o kluczu tajnym, symetrycznym, wspólnym
- Szyfry asymetryczne mają dwa klucze
  - publiczny dostępny dla każdego kto chce zaszyfrować wiadomość do odbiorcy
  - prywatny znany tylko odbiorcy, pozwalający na odszyfrowanie wiadomości

Szyfry asymetryczne sposób postępowania

(kroki wstępne przeprowadzone przez Alicję)

- Alicja generuje klucz swoją parę kluczy: publiczny i prywatny
- Klucz publiczny zostaje ogłoszony do wiadomości wszystkich potencjalnie zainteresowanych

(wysyłanie zaszyfrowanej informacji do Alicji)

- Bolek odszukuje klucz publiczny Alicji
- Szyfruje dane do Alicji jej kluczem publicznym i wysyła do niej
- Tylko Alicja, posiadająca klucz prywatny jest w stanie odszyfrować wiadomość od Bolka

Algorytm Diffiego-Hellmana (zarys)

- Czy zawsze trzeba uzgodnić wcześniej klucze aby móc komunikować się w sposób bezpieczny?
- Czy można zrealizować coś takiego w oparciu o operacje matematyczne

Algorytm Diffiego-Hellmana (zarys)

- Alicja wysyła list do Bolka w zamkniętej szkatułce z własną kłódką
- Bolek dokłada swoją kłódkę i odsyła szkatułkę
- Alicja zdejmuje swoją kłódkę … ale wiadomość nadal jest chroniona kłódką Bolka
- Bolek zdejmuje swoją kłódkę i odczytuje list

Algorytm Diffiego-Hellmana (zarys)

- Pierwiastek pierwotny modulo p, to liczba której potęgi generują wszystkie niezerowe liczby mod p, np. 5 jest pierwiastkiem pierwotnym modulo 7
- $5^1 (\text{mod } 7) = 5$
- $5^2 (\text{mod } 7) = 4$
- $5^3 (\text{mod } 7) = 6$
- $5^4 (\text{mod } 7) = 2$
- $5^5 (\text{mod } 7) = 3$
- $5^6 (\text{mod } 7) = 1$

Przy takim założeniu zawsze można będzie rozwiązać równanie
$y=5^x \text{ (mod } 7)$

Algorytm Diffiego-Hellmana (zarys)

- Znane są liczby g i p, gdzie g jest pierwiastkiem pierwotnym
- Alicja losuje wartość XA, która jest jej kluczem prywatnym
- $Y^A = g^{XA}$ jest jej kluczem publicznym
- Bolek postępuje analogicznie

Algorytm Diffiego-Hellmana (zarys)

- Alicja chce wysłać wiadomość do Bolka
- Odszukuje jego klucz publiczny i oblicza

$K=(Y^B)^{XA}$

- Szyfruje wiadomość za pomocą klucza K

- Bolek odbiera wiadomość i odszukuje klucz publiczny Alicji
- Oblicza $(Y^A)^{XB}=(g^{XA})^{XB}=(g^{XB})^{XA}=(Y^B)^{XA}=K$

RSA (zarys)

- Kluczem publicznym jest
  - Liczba N = p*q, gdzie p i q są dużymi liczbami pierwszymi
  - Liczba e, nie mająca wspólnych dzielników z (p-1) i (q-1)
- Kluczem prywatnym są liczby p i q oraz liczba d taka, że d*e = 1 mod ϕ(N), gdzie ϕ(N) to funkcja Eulera obliczana jak (p-1)*(q-1)

RSA (zarys)

- Szyfrowanie

  $C = M^e \bmod N$

- Odszyfrowywanie

  $M = C^d \bmod N$

Szyfry asymetryczne

- Na czym polega bezpieczeństwo szyfru?
- Na uzależnieniu wiarygodności szyfru od TRUDNOŚCI rozwiązania pewnego problemu matematycznego
  - rozkładu na czynniki pierwsze – RSA
  - problemowi logarytmu dyskretnego - algorytm Diffiego-Hellmana

Porównanie cech szyfrów symetrycznych i asymetrycznych

- Największa wada szyfrów symetrycznych związana jest z problemem dystrybucji oraz tajności klucza
  - Jeśli wykorzystujemy jeden tajny klucz, jego ujawnienie osłabia bezpieczeństwo całego systemu
  - Jeśli każda komunikująca się para posiada własny klucz, liczba kluczy rośnie zgodnie z wzorem

N*(N-1)/2

Porównanie cech szyfrów symetrycznych i asymetrycznych

- Praktyczna realizacja transportu kluczy w wojsku (NSA, NATO)

http://en.wikipedia.org/wiki/AN/CYZ-10

„… the KYK-13 is still used widely today (2012) …”
http://www.cryptomuseum.com/crypto/usa/kyk13/

Porównanie cech szyfrów symetrycznych i asymetrycznych

- Największą wadą szyfrów asymetrycznych jest prędkość działania
  - szyfry asymetryczne wykorzystują potęgowanie modulo bardzo dużych liczb (o długości 512 – 4096 bitów)
- Szyfry symetryczne zwykle wykorzystują proste operacje arytmetyki modulo 2 oraz odwołania do pamięci (np. budowa S-box-ów), świetnie dają się implementować w sprzęcie
- W zależności od implementacji (software/hardware) szyfry symetryczne mogą być nawet do 1000 razy szybsze

Szyfr hybrydowy

- Szyfr hybrydowy łączy najlepsze cechy szyfrów symetrycznych i asymetrycznych
  - szybkość szyfrowania symetrycznego
  - szyfry asymetryczny, który rozwiązuje problem dystrybucji klucza

Szyfr hybrydowy sposób postępowania

- Generacja losowego klucza symetrycznego
- Zaszyfrowanie danych kluczem symetrycznym
- Pobranie klucza publicznego odbiorcy
- Zaszyfrowanie kluczem publicznym odbiorcy, klucza symetrycznego i dołączenie do zaszyfrowanych danych

Tryby pracy algorytmów blokowych

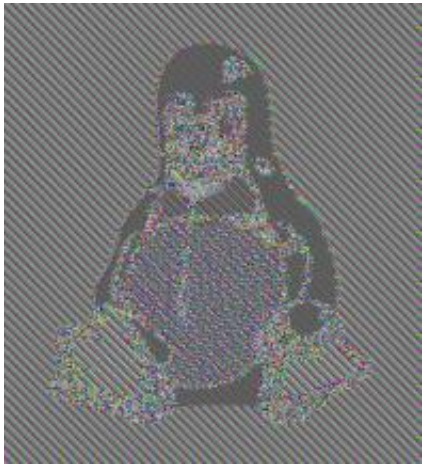
- Szyfry blokowe działają na blokach o długości 8 lub 16 bajtów
- W jaki sposób zaszyfrować większe dane – trzeba wielokrotnie szyfrować poszczególne bloki i dla bezpieczeństwa dokonywać pewnych powiązań

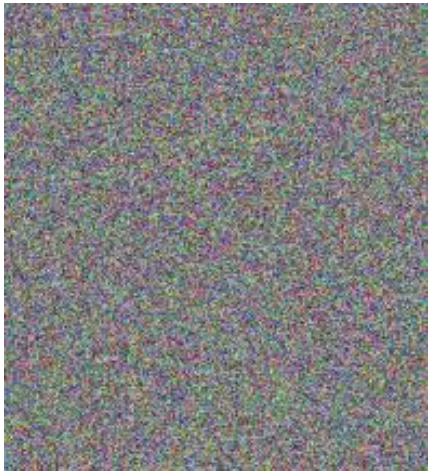
Tryby pracy algorytmów blokowych

- Elektroniczna książka kodowa (ang. electronic code book, ECB)
- Wiązanie bloków zaszyfrowanych (ang. cipher block chaining, CBC)
- Wyjściowe sprzężenie zwrotne (ang. output feedback, OFB)
- Tryb licznikowy (ang. counter mode, CTR)
- Sprzężenie zwrotne szyfrogramu (ang. cipher feedback mode, CFB)

Elektroniczna książka kodowa

- Każdy blok danych szyfrowany jest niezależnie od innych
- Identyczne dane występujące w tekście jawnym dadzą powtarzalny wzorzec w szyfrogramie

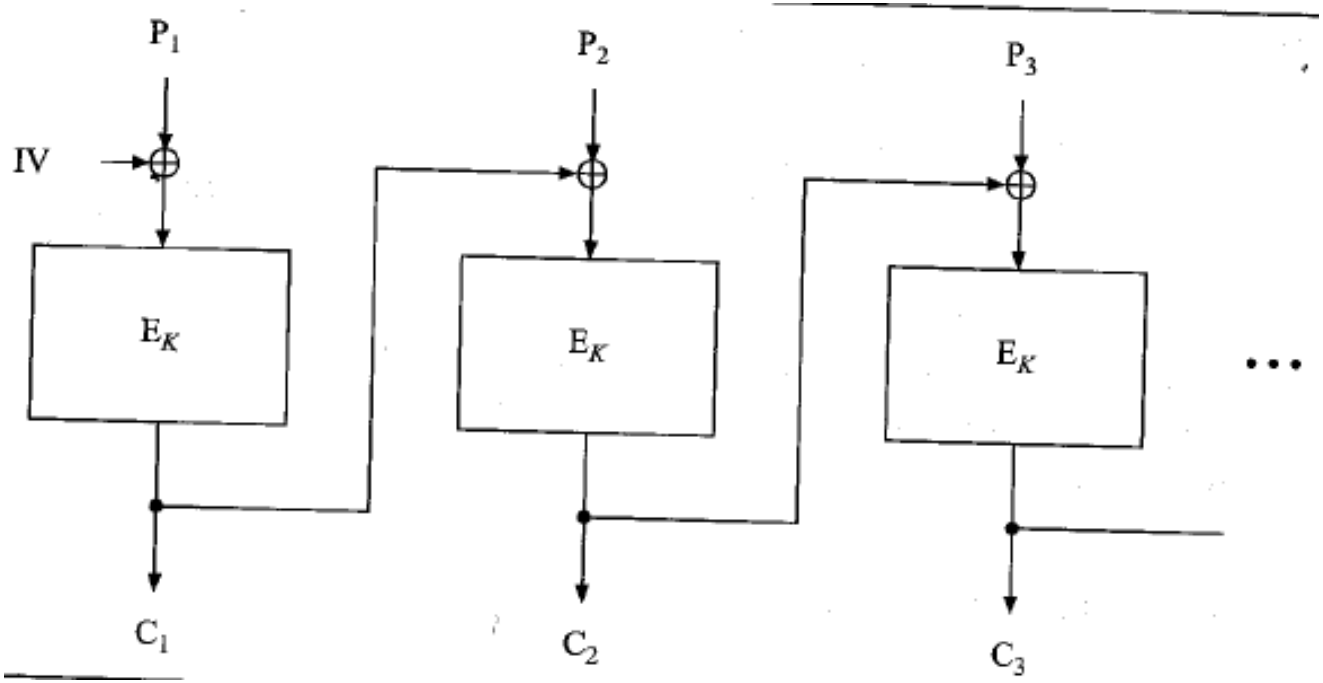




Rysunki. Wikipedia

Wiązanie bloków zaszyfrowanych

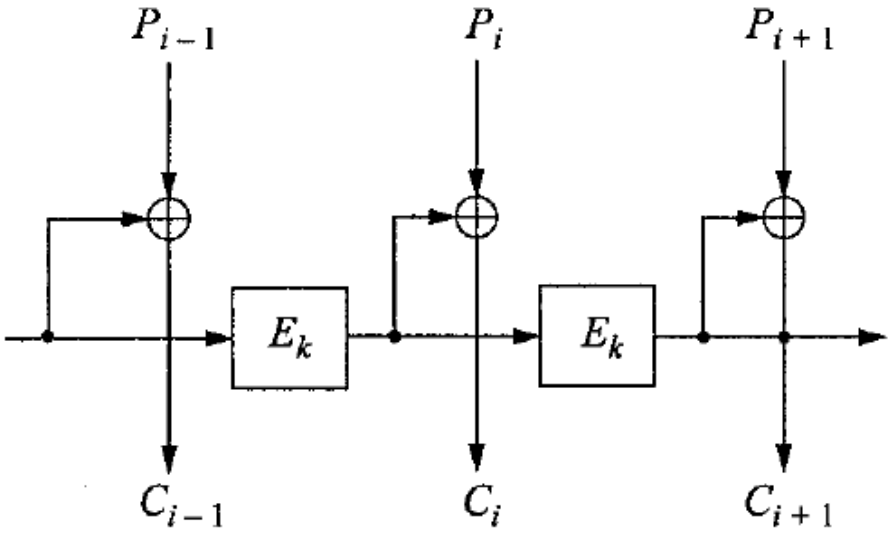
- Wiązanie następnego bloku z poprzednim poprzez dokonanie operacji XOR z Ci i Mi+1



Rysunek. Ross Anderson, Inżynieria zabezpiecze

Wyjściowe sprzężenie zwrotne

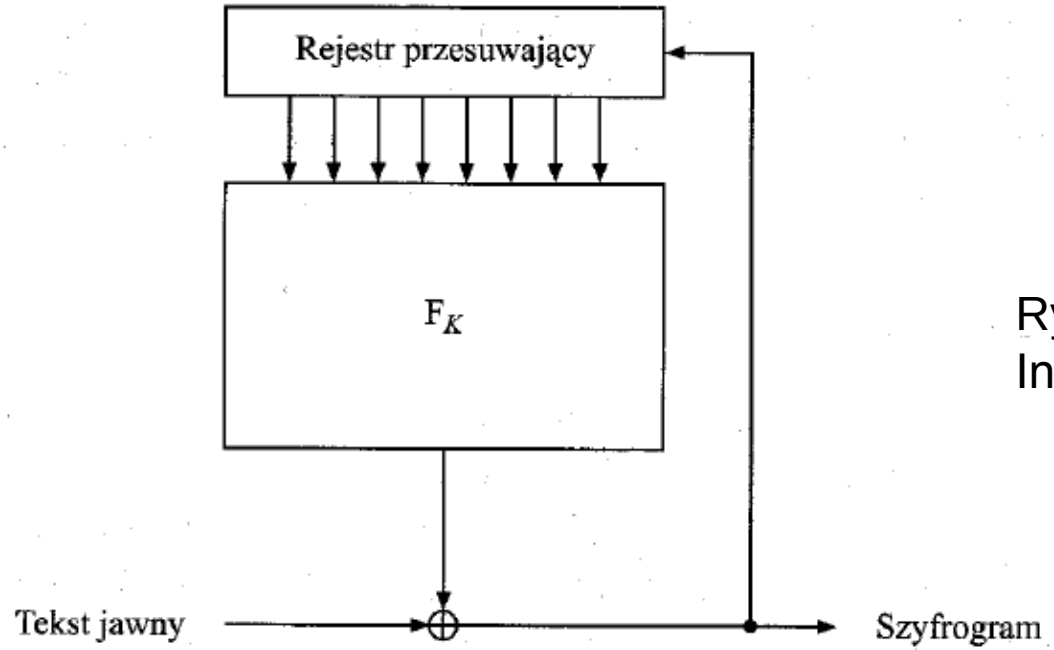
- Szyfr strumieniowy, zbudowany w oparciu o wielokrotne szyfrowanie klucza i wiązanie wyniku za pomocą funkcji xor z danymi do zaszyfrowani



Rysunek. Bruce Schneier, Kryptografia dla praktyków

Sprzężenie zwrotne szyfrogramu

- Szyfr strumieniowy w oparciu o szyfrowanie rejestru przesuwnego zależnego od wyniku poprzedniego szyfrowania



Rysunek. Ross Anderson, Inżynieria zabezpieczeń

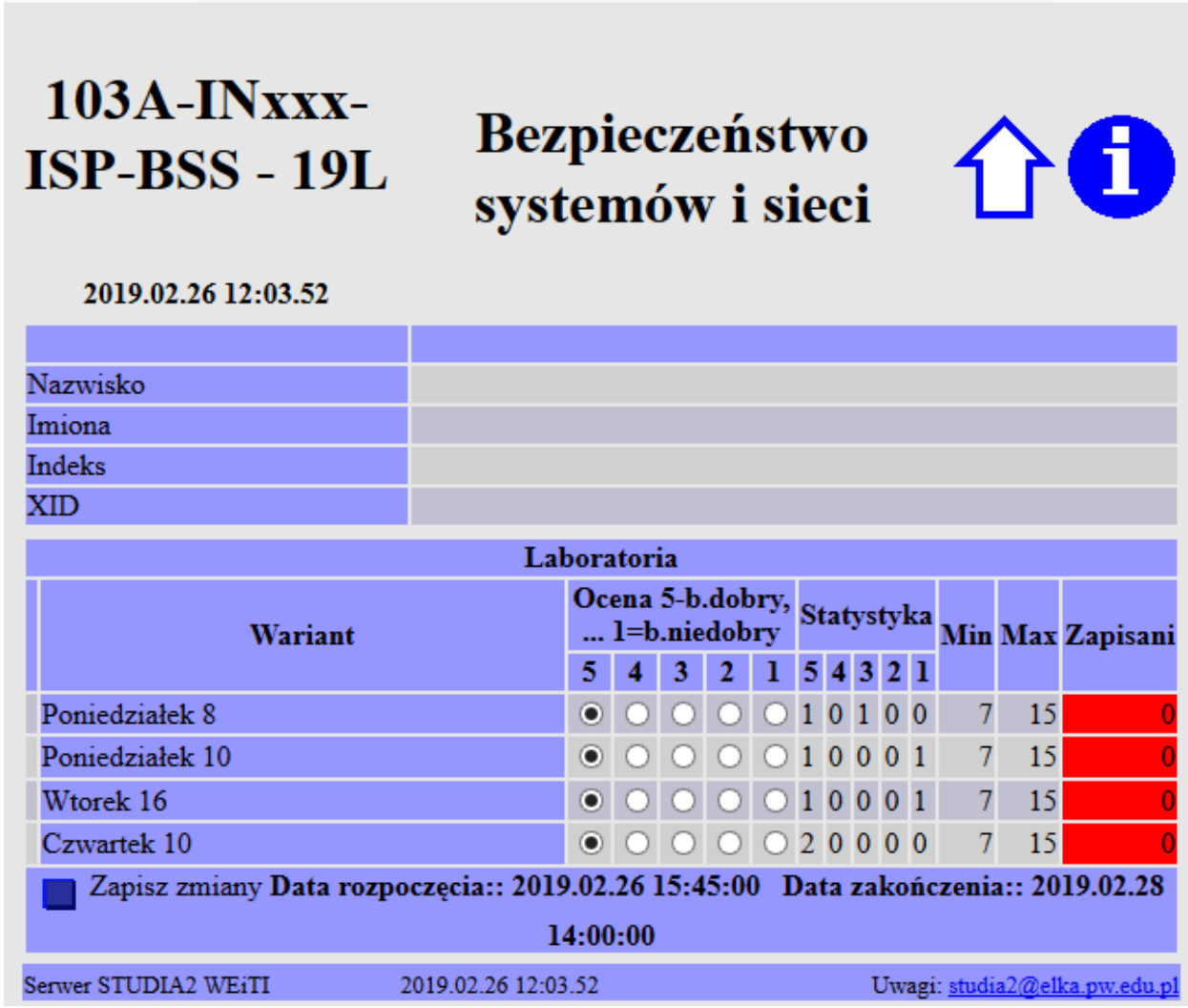
Zapisy na laboratorium

- W związku z liczbą zapisanych - 52 osoby - oraz preferencjami z ankiety zostaną uruchomione 4 terminy
  - poniedziałek 8:15-10:00
  - poniedziałek 10:15-12:00
  - wtorek 16:15-18:00
  - czwartek 10:15-12:00

Uwaga – zajęcia nie są co 2 tygodnie !!!

Tydzień	Terminy zajęć	Temat ćwiczenia/inne informacje
Luty (18-22)		
Luty/Marzec (25-1)		
Marzec (4-8)		
Marzec (11-15)		
Marzec (18-22)		
Marzec (25-29)	25, 26 i 28	***Algorytmy szyfrowania***
Kwiecień (1-5)		
Kwiecień (8-12)	8, 9 i 11	***Openssl***
Kwiecień (15-17)	15, 16	***GPG***
Kwiecień (24-26)	25	***GPG***
Kwiecień (29-30)		
Maj (6-10)	6, 7 i 9	***Stunnel***
Maj (13-16)	13, 14 i 16	***Systemy IDS***
Maj (20-24)		
Maj (27-31)		***Bezpieczeństwo serwisów internetowych***
Czerwiec (3-7)	4, 5 i 7	***Bezpieczeństwo aplikacji***
Czerwiec (10-12)		1 (!!!) termin dodatkowy, ustalony z zainteresowanymi
Czerwiec (13-15)		Sesja
Czerwiec (17-22)		Sesja
Czerwiec (24-29)		Sesja

Zapisy w systemie Studia vel Eres



103A-INxxx-ISP-BSS - 19L

Bezpieczeństwo systemów i sieci

2019.02.26 12:03.52

Nazwisko	
Imiona	
Indeks	
XID	

Laboratoria

Wariant	Ocena 5-b.dobry, ... 1=b.niedobry					Statystyka					Min	Max	Zapisani
	5	4	3	2	1	5	4	3	2	1			
Poniedziałek 8	◉	○	○	○	○	1	0	1	0	0	7	15	0
Poniedziałek 10	◉	○	○	○	○	1	0	0	0	1	7	15	0
Wtorek 16	◉	○	○	○	○	1	0	0	0	1	7	15	0
Czwartek 10	◉	○	○	○	○	2	0	0	0	0	7	15	0

Zapisz zmiany **Data rozpoczęcia:: 2019.02.26 15:45:00 Data zakończenia:: 2019.02.28 14:00:00**

Serwer STUDIA2 WEiTI 2019.02.26 12:03.52 Uwagi: studia2@elka.pw.edu.pl

Zapisy w systemie Studia vel Eres

- Zapisy będą możliwe w terminie
  - od 2019.02.26 15:45 (dzisiaj, po zajęciach)
  - do 2019.02.18 14:00 (najbliższy czwartek)
- Proszę podać ***co najmniej 3*** terminy w kolejności od najbardziej dogodnego 5 do najmniej dogodnego - 1 oznacza termin nie wskazany
- Jeśli ktoś nie może podać 3 terminów proszę o dodatkowego maila z wyjaśnieniem ***z jakimi przedmiotami kolidują*** terminy laboratorium BSS