



# *Kryptografia*

Janusz Szwabiński

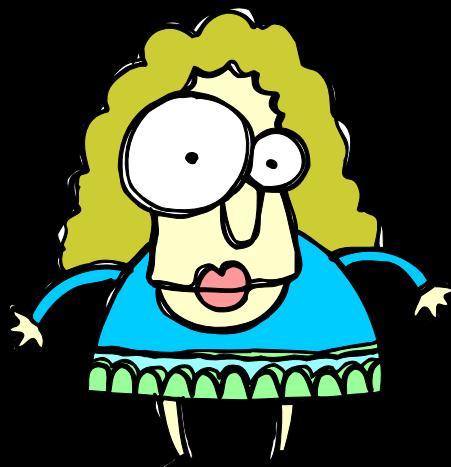
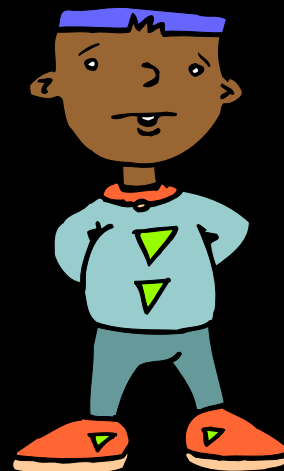
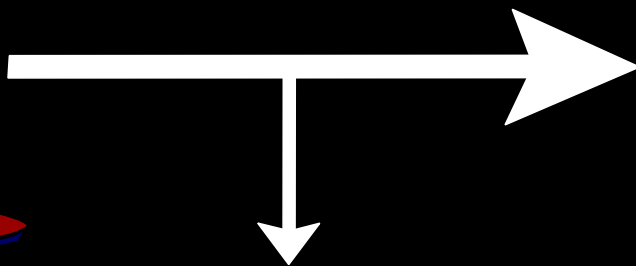
`szwabin@ift.uni.wroc.pl`

Instytut Fizyki Teoretycznej UWr



## *Plan wykładu*

- Pojęcia podstawowe
- Szyfry historyczne
- Współczesne metody szyfrowania informacji
  - algorytmy z kluczem symetrycznym
  - algorytmy z kluczem publicznym
- GnuPG: szyfrujemy własną pocztę elektroniczną





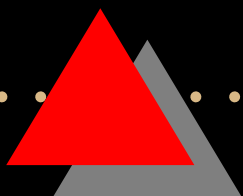
## *Pojęcia podstawowe*

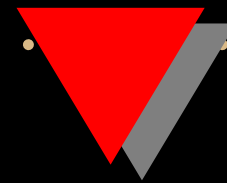
**Steganografia** ukrywanie tajnych wiadomości

**Kryptografia** dziedzina wiedzy zajmująca się  
zabezpieczaniem wiadomości

**Kryptoanaliza** sztuka łamania szyfrów

**Kryptologia** dziedzina matematyki obejmująca  
kryptografię i kryptoanalizę

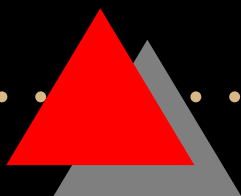




**Szyfry podstawieniowe** każdy znak w tekście jawnym zastępowany jest innym znakiem

**Szyfry przestawieniowe** wszystkie znaki tekstu jawnego pojawiają się w tekście zaszyfrowanym w zmienionej kolejności

**Algorytm ograniczony** bezpieczeństwo algorytmu oparte jest na utrzymaniu w tajemnicy jego istoty





## Szyfr Cezara

Prosty szyfr podstawieniowy:

ABCDEFGHIJKLMNOPQRSTUVWXYZ

DEFGHIJKLMNOPQRSTUVWXYZABC

Tekst jawny: K R Y P T O G R A F I A

Szyfrogram: N U B T Y S J U D I L D



## *Szyfr Cezara okiem matematyka*

- kolejnym literom alfabetu łacińskiego przyporządkowujemy liczby od 0 do 25
- szyfrowanie

$$C = (P + k) \bmod 26$$

- deszyfrowanie

$$P = (C - k) \bmod 26$$



## *Szyfr Vigenère'a (XVI w)*

Tekst jawny: K R Y P T O G R A F I A

Klucz: K L U C Z K L U C Z K L

ABCDEFGHIJKLMNOPQRSTUVWXYZ  
KLMNOPQRSTUVWXYZABCDEFGHIJ  
LMNOPQRSTUVWXYZABCDEFGHIJK  
UVWXYZABCDEFGHIJKLMNOPQRST  
CDEFGHIJKLMNOPQRSTUVWXYZAB  
ZABCDEFGHIJKLMNOPQRSTUVWXY

Szyfrogram: U C S R S Y R L C E S L



## *Enigma (maszyna rotorowa)*



- maszyna realizująca szyfr Vigenère'a
- szyfr złamany w latach 30. przez M. Rejewskiego, J. Różyckiego i H. Zygalskiego



## *Kolumnowy szyfr przestawieniowy*

Tekst jawny: informatyka na wydziale fizyki i astronomii

i	n	f	o	r	m
a	t	y	k	a	n
a	w	y	d	z	i
a	l	e	f	i	z
y	k	i	i	a	s
t	r	o	n	o	m
i	i				

Szyfrogram: iaaaytintwlkrifyyeiookdfinraziaomnizsm





## Szyfr Vernama (*one-time pad*)

Tekst jawny ('b'):      1   1   0   0   0   1   0

Klucz ('#'):              0   1   0   0   0   1   1

Szyfrogram (XOR):    1   0   0   0   0   0   1

Szyfr bezwarunkowo bezpieczny, jeśli:

- klucz jest ciągiem losowym
- klucz jest jednorazowy
- długość klucza jest co najmniej równa długości szyfrowanego tekstu



## Problemy

- wygenerowanie losowego klucza
- całkowicie bezpieczne przesłanie tego klucza

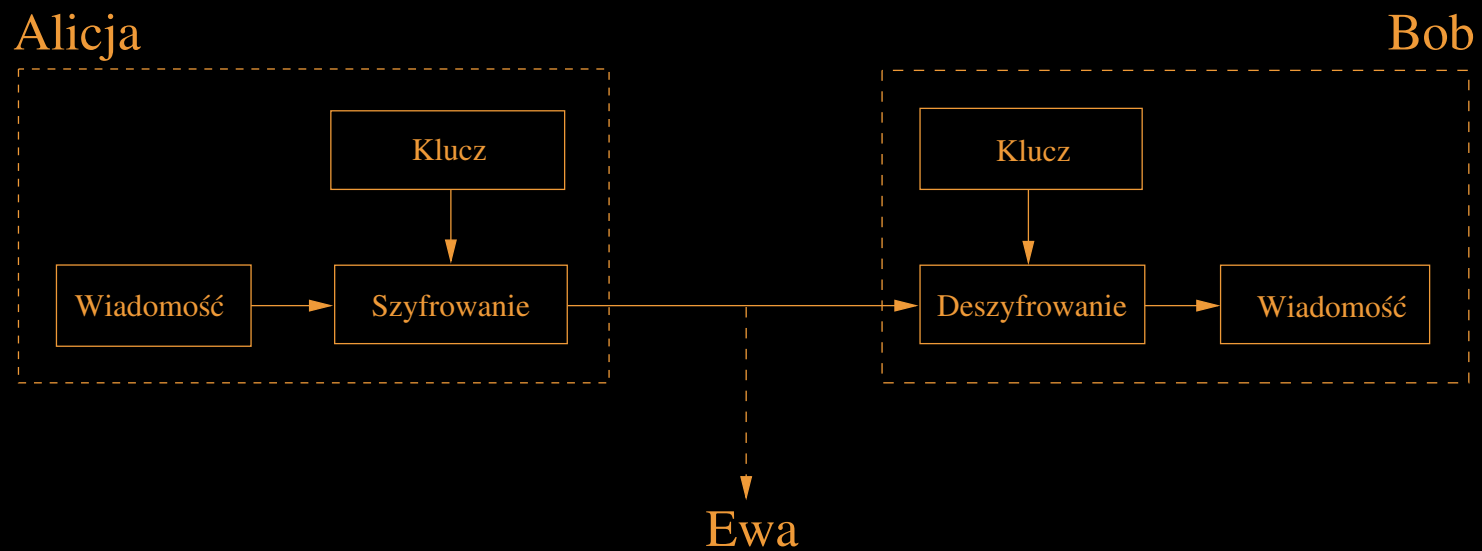


## *Współczesne metody szyfrowania informacji*

**algorytmy symetryczne** klucz szyfrujący wyznaczany jest z klucza deszyfrującego i odwrotnie, np. DES

**algorytmy z kluczem publicznym** klucz stosowany do szyfrowania jest inny niż klucz stosowany do deszyfrowania (przy tym jeden nie może być wyznaczony z drugiego w rozsądnym czasie), np. RSA

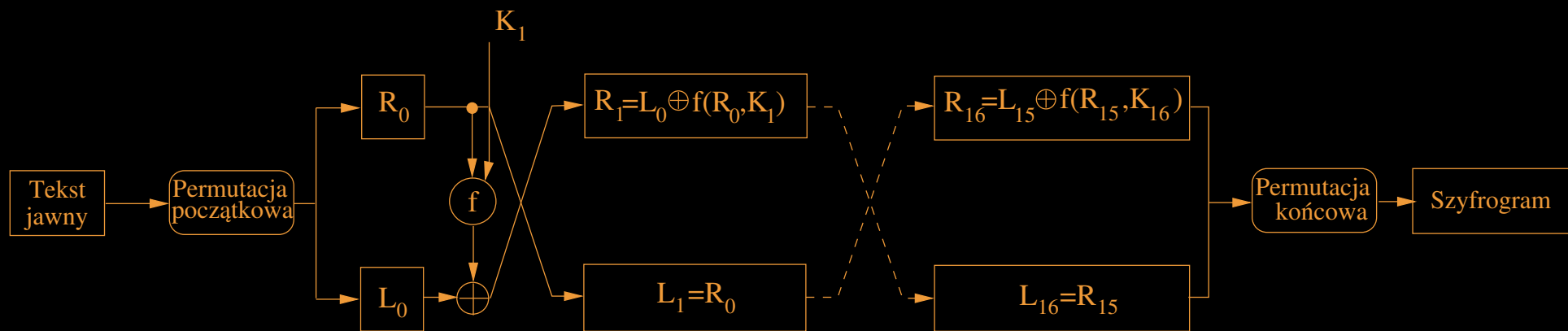
# Wymiana informacji przy użyciu kryptografii symetrycznej





## *Algorytm DES*

- IBM/NSA, 1974
- standard federalny w USA, 1976
- szyfr blokowy (dług. bloku - 64 bity)
- klucz o długości 56 bitów
- ten sam algorytm do szyfrowania i deszyfrowania (kombinacja mieszania i rozpraszania)

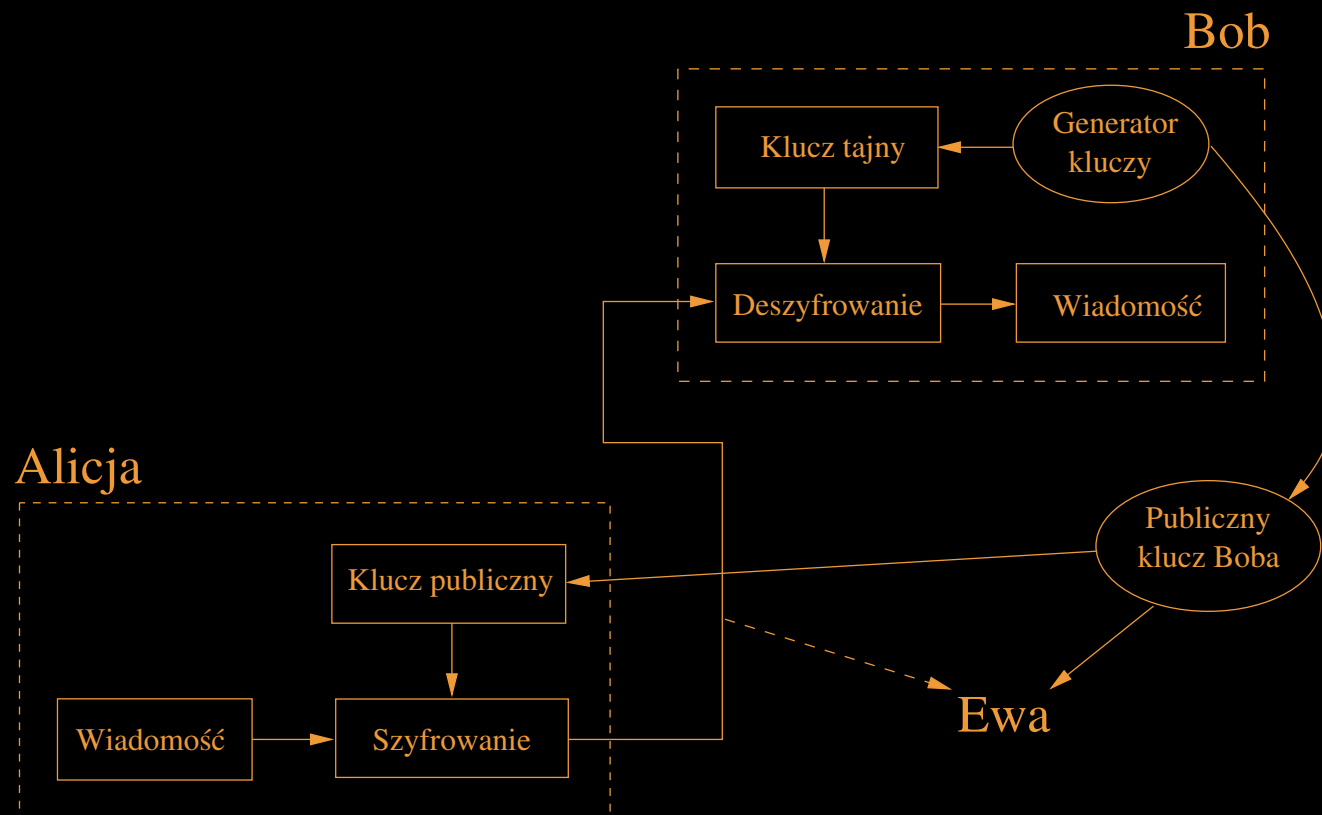




## Przeciętny czas realizacji sprzętowego łamania brutalnego:

Koszt	Długość klucza w bitach					
	40	56	64	80	112	128
$10^5 \$$	2 s	35 h	1 rok	70 000 lat	$10^{14}$ lat	$10^{19}$ lat
$10^6 \$$	0,2 s	3,5 h	37 dni	7000 lat	$10^{13}$ lat	$10^{18}$ lat
$10^7 \$$	0,02 s	21 min	4 dni	700 lat	$10^{12}$ lat	$10^{17}$ lat
$10^8 \$$	2 ms	2 min	9 h	70 lat	$10^{11}$ lat	$10^{16}$ lat
$10^9 \$$	0,2 ms	13 s	1 h	7 lat	$10^{10}$ lat	$10^{15}$ lat
$10^{10} \$$	0,02 ms	1 s	5,4 min	245 dni	$10^9$ lat	$10^{14}$ lat
$10^{11} \$$	$2 \mu s$	0,1 s	32 s	24 dni	$10^8$ lat	$10^{13}$ lat
$10^{12} \$$	$0,2 \mu s$	0,01 s	3 s	2,4 dni	$10^7$ lat	$10^{12}$ lat
$10^{13} \$$	$0,02 \mu s$	1 ms	0,3 s	6 h	$10^6$ lat	$10^{11}$ lat

# Wymiana informacji przy użyciu kryptografii z kluczem publicznym






## Algorytm RSA

- Clifford Cocks, 1973
- Whitfield Diffie i Martin Hellman, 1976
- Ronald Rivest, Adi Shamir i Leonard Adleman, 1977
- oferuje szyfrowanie wiadomości i podpis elektroniczny

Generowanie pary kluczy:

1. weź dwie duże liczby pierwsze,  $p$  i  $q$
  2. oblicz  $n = p * q$
  3. oblicz  $m = (p - 1)(q - 1)$
  4. wybierz losowo małą liczbę  $e$ , względnie pierwszą z  $m$
- 



5. znajdź liczbę  $d$  taką, że

$$\begin{aligned} de &= 1 \bmod m \\ d &= \frac{1 + km}{e}, \quad k \in \mathbb{Z} \end{aligned}$$

6. opublikuj parę  $(n, e)$

7. dobrze schowaj  $d$

8. zniszcz  $p$  i  $q$

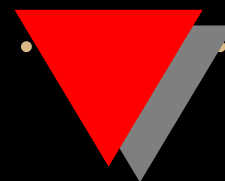


Szyfrowanie (wiadomość - liczba mniejsza od  $n$ )

$$C = P^e \bmod n$$

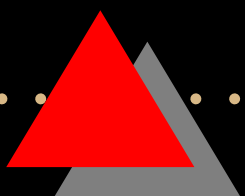
Deszyfrowanie

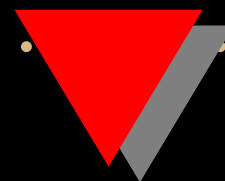
$$P = C^d \bmod n$$



## Bezpieczeństwo:

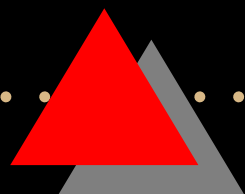
- algorytm nie gwarantuje pełnego bezpieczeństwa
- złamanie szyfru wymaga efektywnego algorytmu faktoryzacji dużych liczb
- taki algorytm faktoryzacji już istnieje (algorytm Shora), jednak wymaga on komputera kwantowego
- badania nad zbudowaniem komputera kwantowego trwają . . .





Zalecane długości klucza publicznego (w bitach) chroniące przed atakiem ze strony:

Rok	osoby prywatnej	firmy	instytucji rządowych
1995	768	1280	1536
2000	1024	1280	1536
2005	1280	1536	2048
2010	1280	1536	2048
2015	1536	2048	2048





## *GNU Privacy Guard (GnuPG)*

- generowanie pary kluczy

```
gpg --gen-key
```

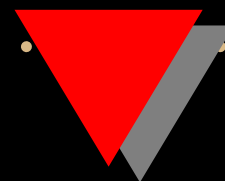
- certyfikat anulowania klucza

```
gpg --gen-revoke USERID > gpg-revoke.txt
```

- opublikowanie klucza publicznego

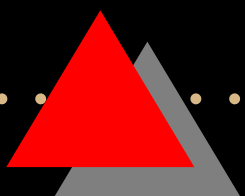
```
gpg -a --export USERID | mail -s "add"  
pgp-public-keys@keys.pl.pgpg.net
```





## Jeśli „nasz” serwer nie działa:

- `pgp-public-keys@keys.pgp.net`
- `pgp-public-keys@keys.uk.pgp.net`
- `pgp-public-keys@keys.de.pgp.net`
- `pgp-public-keys@keys.dk.pgp.net`
- `pgp-public-keys@keys.no.pgp.net`
- `pgp-public-keys@keys.us.pgp.net`
- `pgp-public-keys@keys.nl.pgp.net`
- `pgp-public-keys@keys.fi.pgp.net`
- `pgp-public-keys@keys.es.pgp.net`
- `pgp-public-keys@keys.hr.pgp.net`
- `pgp-public-keys@keys.tw.pgp.net`
- `pgp-public-keys@keys.au.pgp.net`





## Źródła

- Bruce Schneier, „Kryptografia dla praktyków”
- S. Garfinkel, G. Spafford, „WWW. Bezpieczeństwo i handel”
- <http://www.kryptografia.com>
- <http://www.gnupg.org>