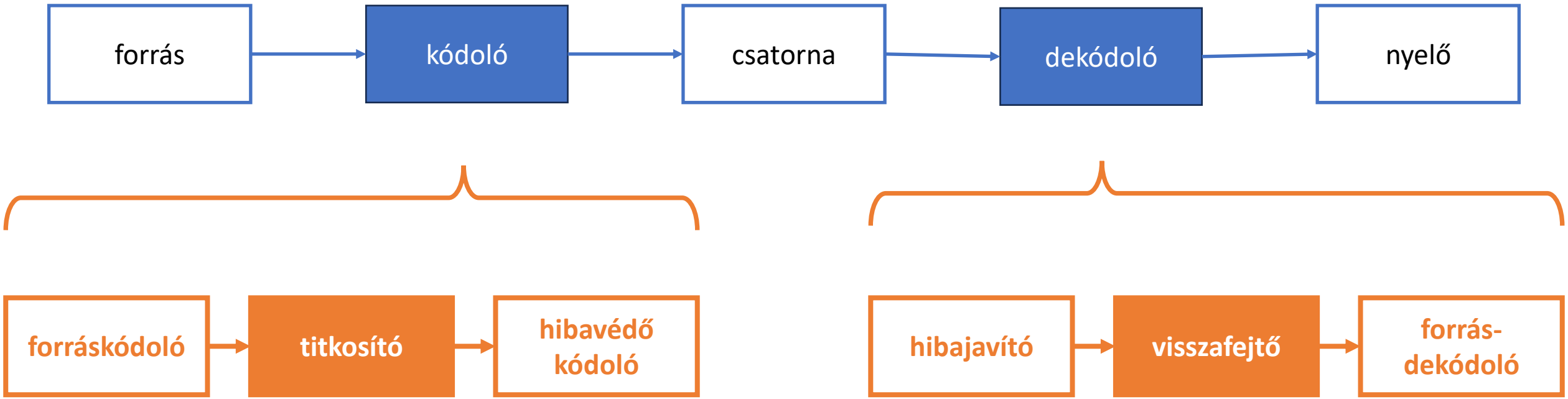
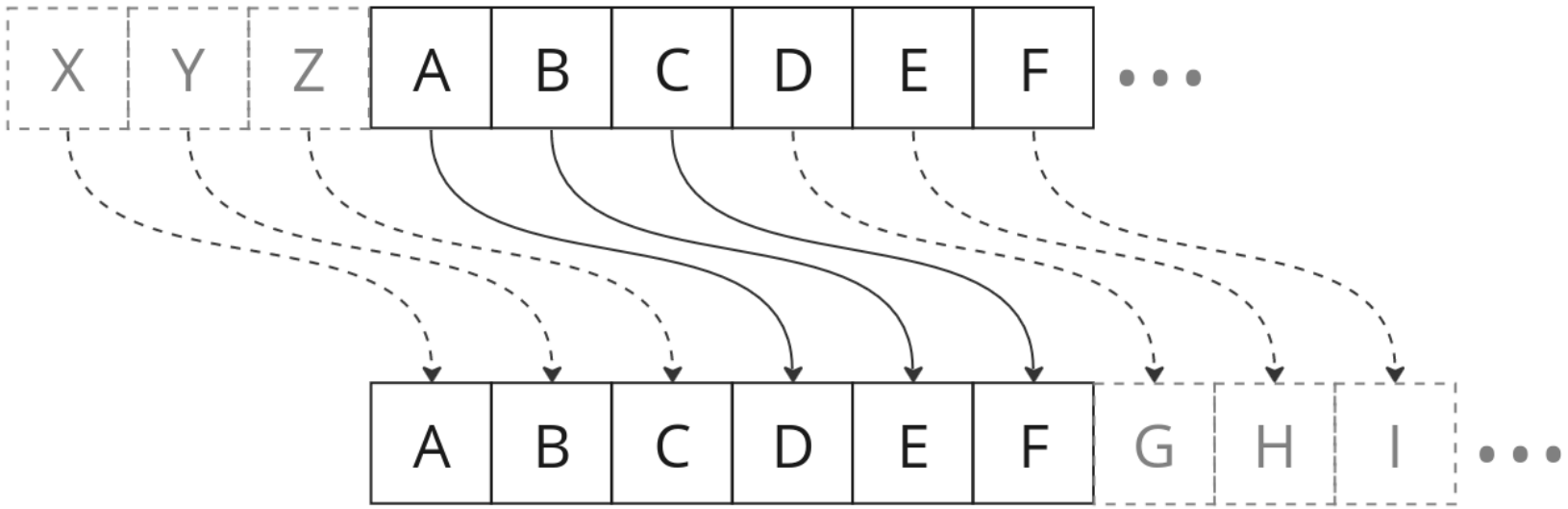

forrás
kódoló
csatorna
dekódoló
nyelő
forráskódoló
titkosító
hibavédő kódoló
hibajavító
visszafejtő
forrás-dekódoló

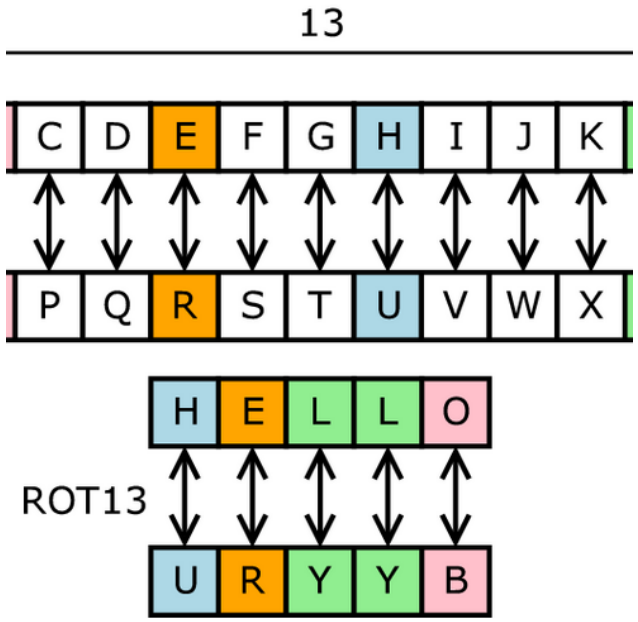

Eve
Titkosítás
Alice
Bob

Caesar rejtjelező



Monoalfabetikus rejtjelező

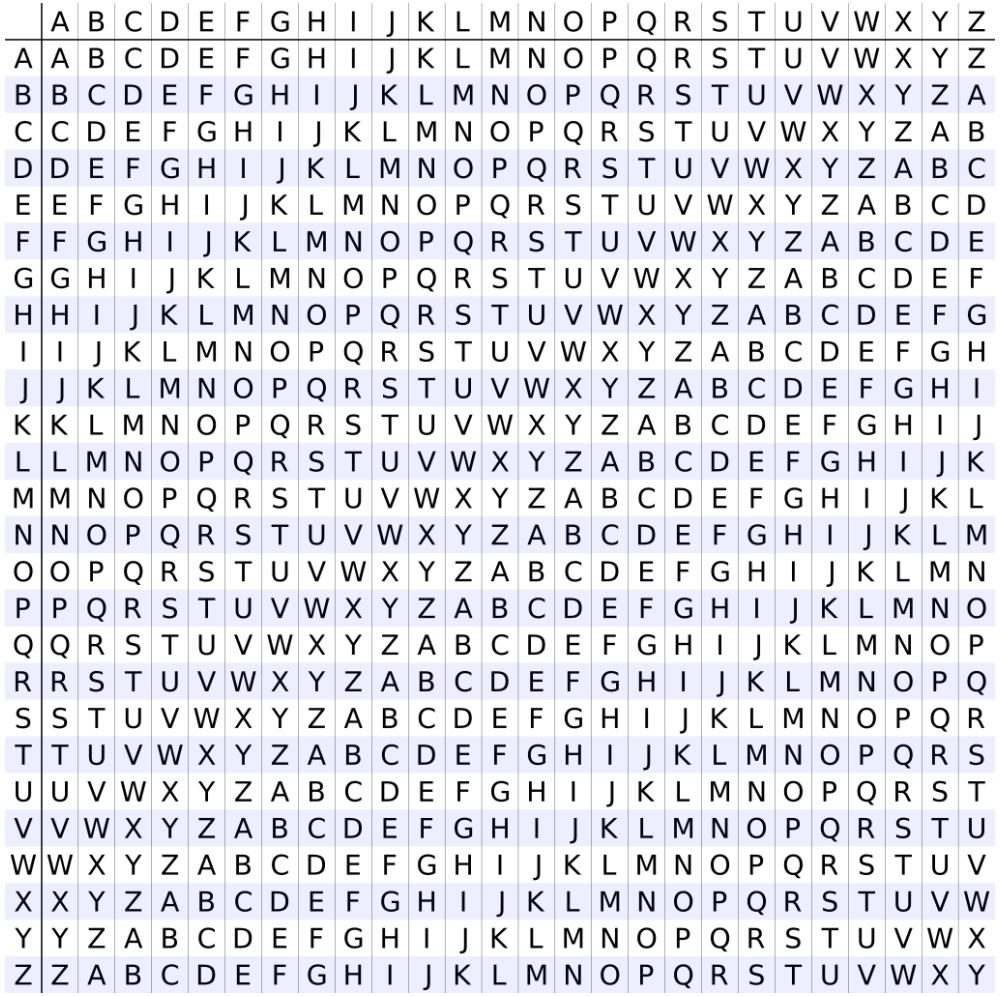
- eltolásos rejtjelező
  - $c = (m + k) \bmod N$
  - $k = 3$ esetében Caesar rejtjelező
- permutációs rejtjelező
- affin rejtjelező
  - $c = (a \cdot m + b) \bmod N$



†m a nyílt üzenet; c a titkosított üzenet; k a kulcs; N az ábécé mérete

A Vigenère rejtjelező

- Giovan Battista Bellaso, 1553
  - később tévesen Blaise de Vigenère-nek tulajdonították, és mind a mai napig az ő nevét viseli
- „le chiffre indéchiffrable”
  - „feltörhetetlen kód”
  - az amerikai polgárháborúban a konföderációs seregek is használták ezt a kódolást
    - gyenge kulcsok: *Manchester Bluff*, *Complete Victory*, *Come Retribution*
- Blaise de Vigenère, 1586
  - rövid kulcsszó után az üzenetet a saját betűivel titkosítja



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

Kasiski teszt

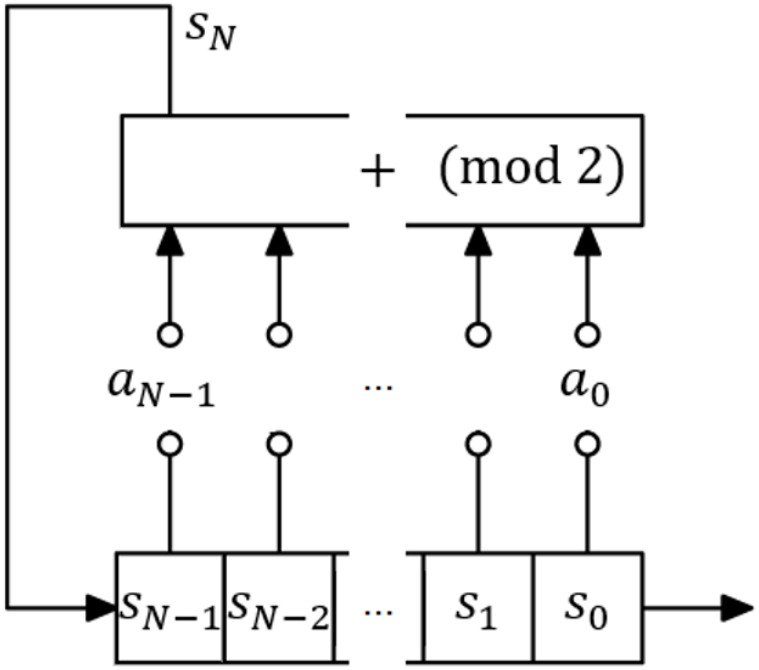
- Vigenère rejtjelező törése
- Friedrich Kasiski, 1863

- kulcs méretének a meghatározása
  - ismétlődő (legalább) 3 hosszú szekvenciák keresése
  - valószínűleg a kulcs ugyanazon részével lettek kódolva
    - minél hosszabb egy ismétlődő szekvencia, ez annál inkább igaz
- törés a betűk előfordulási gyakorisága lapján

LFSR

- álvéletlenszám generálása
- N bites
  - maximum $2^N - 1$ hosszú sorozat
  - de függ a visszacsatolásoktól

- karakterisztikus polinom
  - $K(x) = x^N + \sum_{i=0}^{N-1} a_i x^i$
- Feedback polinom
  - reciprok polinom, azaz:
    - $R(x) = x^N \cdot K(y)|_{y=\frac{1}{x}}$

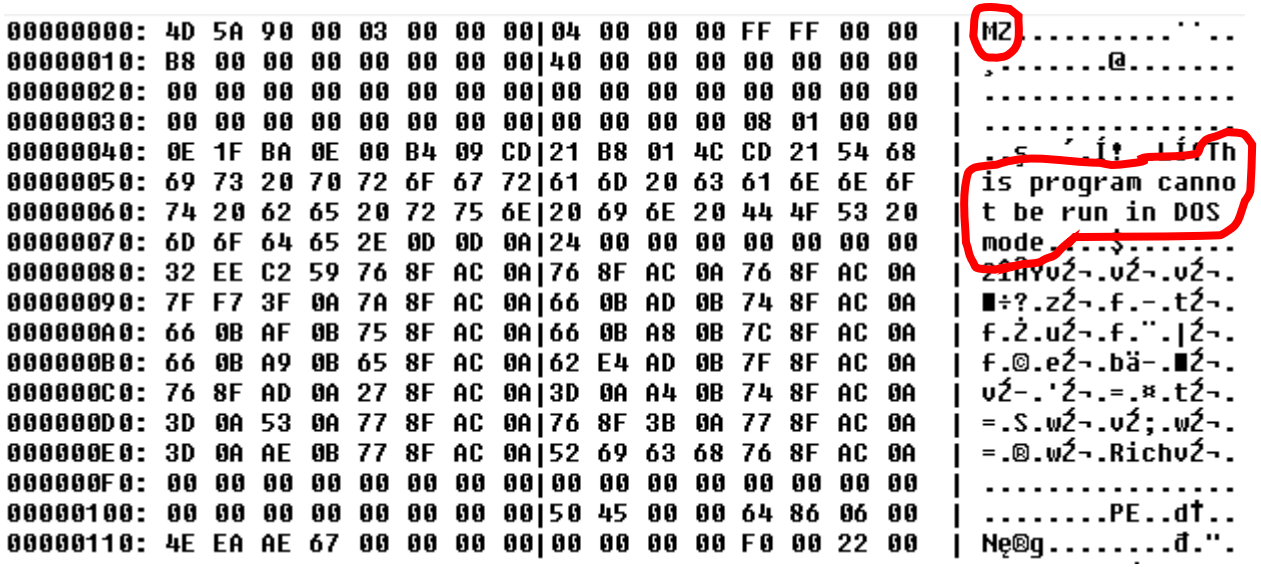


Folyamrejtjelezők

- kis kulcsból nagy mennyiségű kvázi-véletlenszerű adatot generálnak
  - pl. LFSR-rel, ahol a kulcs a visszacsatolás
- titkosítás: az LFSR kimenete XOR a nyílt üzenet
- visszafejtés: az LFSR kimenete XOR a titkosított üzenet

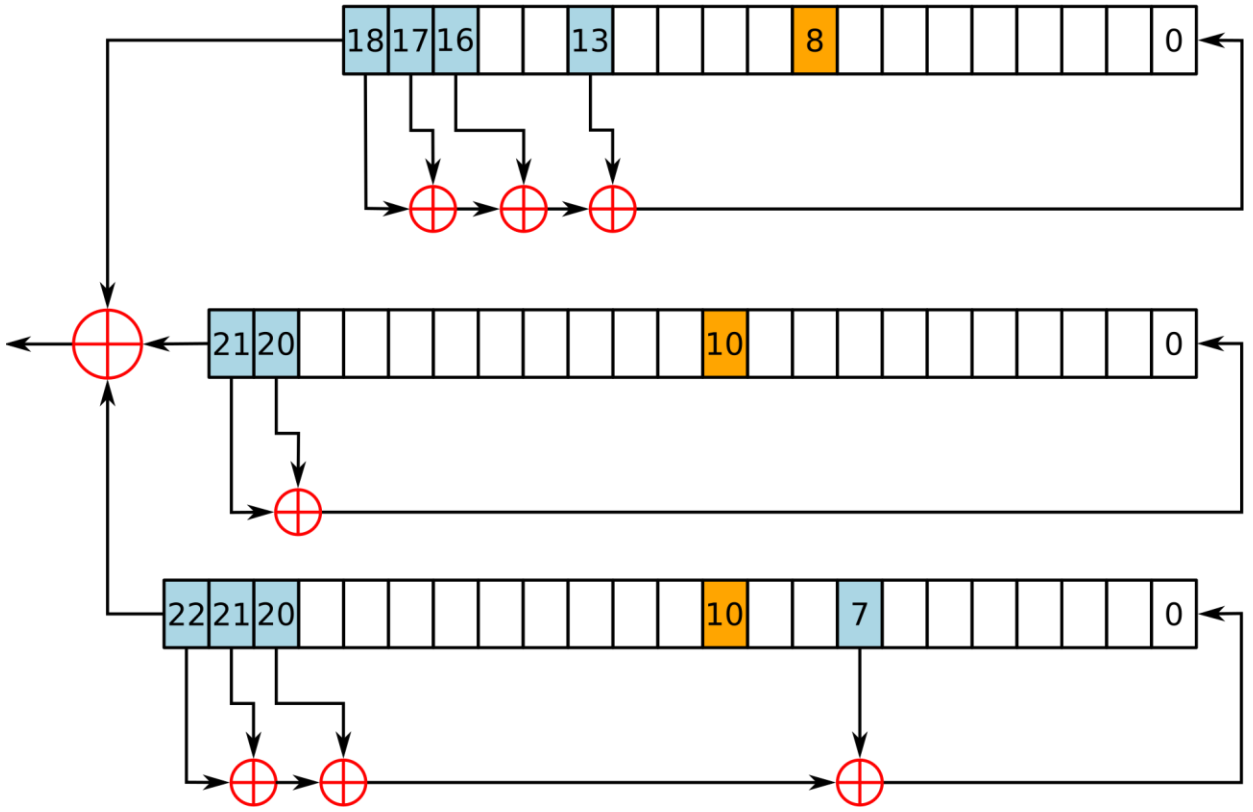
LFSR feltörése

- egy N bites LFSR visszacsatolása meghatározható $2 \cdot N$ bit hosszú nyílt szöveg és a hozzá tartozó titkosított szöveg ismeretében



LFSR felhasználása

- GSM A5/1
  - folyamrejtjelező
  - 1987
  - eredetileg titkos, de kiszivárgott, illetve visszafejtették, feltörték



Kerckhoff-féle elv

- Auguste Kerckhoffs (holland kriptográfus)

Egy kriptorendszer biztonságának kizárólag a kulcs titkosságán kell alapulnia, nem pedig az algoritmus vagy a rendszertervezés titkosságán.

Tökéletes titkosítás

- Shannon-fél definíciója:
  - $P\{M = m | C = c\} = P\{M = m\}$
- a titkosítás tökéletes $\Leftrightarrow P\{e_K(m) = c\} = P\{e_K(m') = c\}$
- a titkosítás tökéletes $\Rightarrow |M| \leq |K|$
- One-time-pad (OTP)
  - $M = K = C = \{0,1\}^N$
  - $P\{e_K(m) = c\} = P\{K \oplus m = c\} = P\{K = c \oplus m\} = 2^{-n} \Rightarrow$ tökéletes

‡*Az oldalon szereplő tételek csak vázlatosan kerültek itt leírásra! Bővebben az előadáson szerepeltek.*

Blokkrejtjelezők

- az adatot fix méretű blokkokra bontja
- titkos kulcs felhasználásával ebből készít ugyanekkora méretű titkosított blokkot

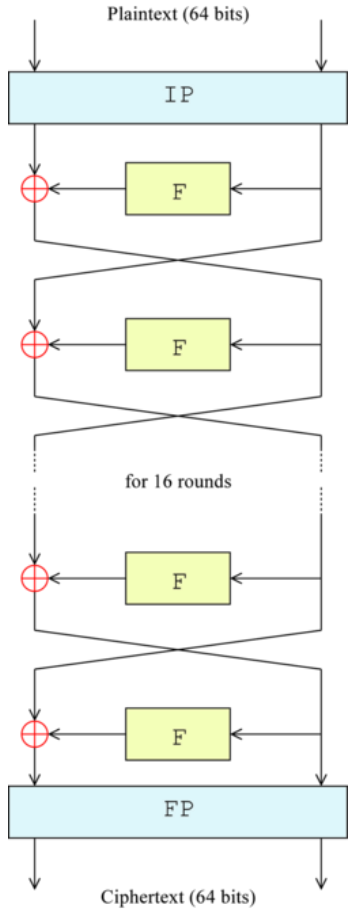
- követelmények:
  - **teljesség**: a kimenet minden bitje minden bemeneti bittől és minden kulcsbittől függjön
  - **statisztikai függetlenség**: ne legyen statisztikai kapcsolat a nyílt blokkok és a titkosított blokkok között
  - **lavina hatás**: a bemenet egy bitjének a megváltoztatására a kimenet minden bitje ½ valószínűséggel változzon meg

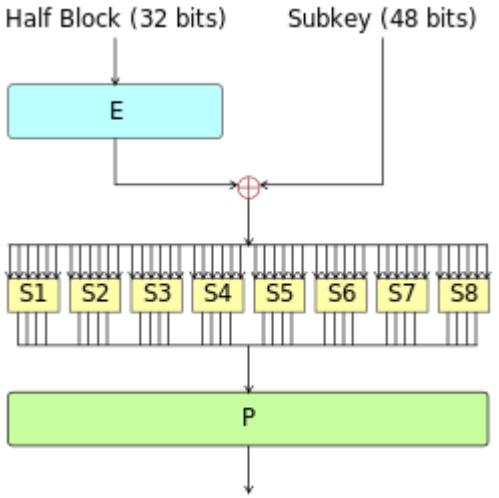
- AES, DES

DES

- az IBM fejlesztette ki a 70-es évekbe
  - Lucifer

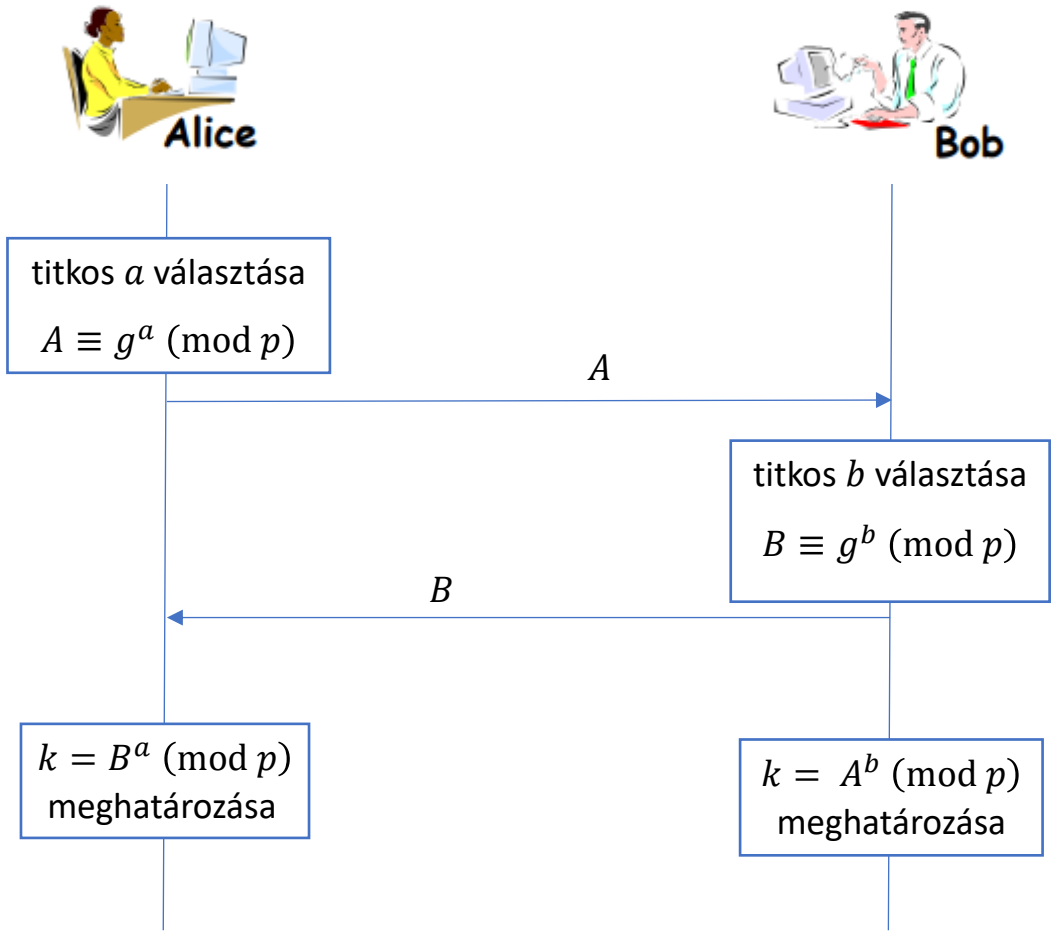
- felépítése:
  - kódoló és dekódoló megegyezik
  - 16 réteg
  - 64 bit be- és kimenet
  - 56 bites kulcs



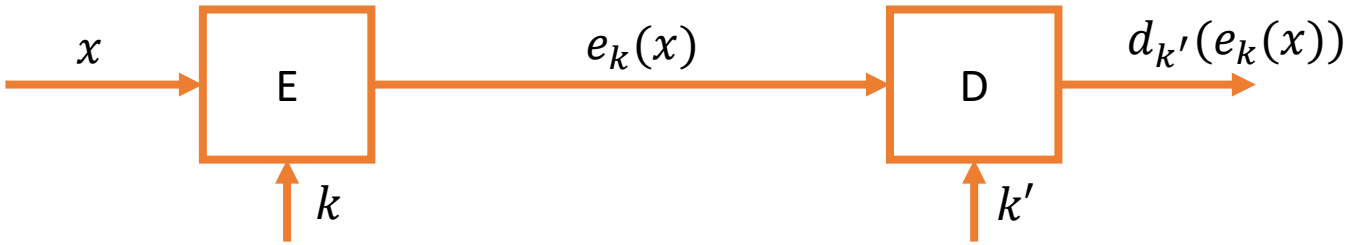


Kulcscsere protokollok

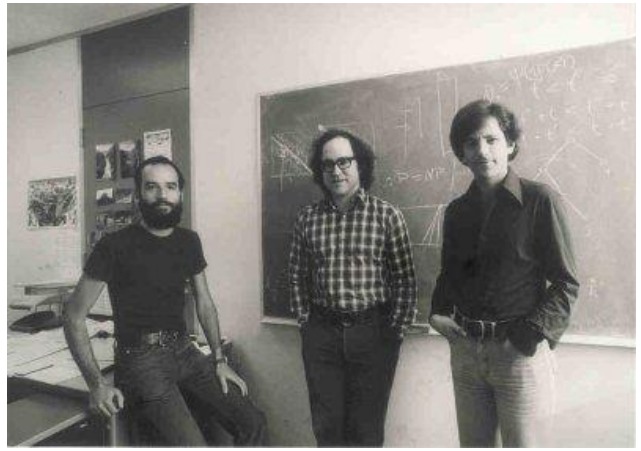
- a titkosító kulcs megosztása
  - két személy olyan módon tudjon megállapodni közös kulcsban, hogy azt harmadik személy ne tudja megszerezni
- Diffie-Hellman kulcscsere
  - első publikált eljárás titkos kulcsok nyilvános cseréjére (1976)
  - támadás: man in the middle



Aszimmetrikus kulcsú titkosítás



- aszimmetrikus kulcsok
  - k' kiszámítása k-ból nehéz feladat
  - k-t nyilvánosságra lehet hozni
- a nyilvános kulcs nem titkos, de a hitelességét biztosítani kell
  - kulcstanúsítványok
- RSA
  - Ronald Rivest, Adi Shamir és Leonard Adleman 1977-ben
  - egy ezzel megegyező algoritmust fejlesztett ki Clifford Cocks 1973-ban
    - a brit Government Communications Headquarters használta titokban
    - csak 1997-ben tehette közzé

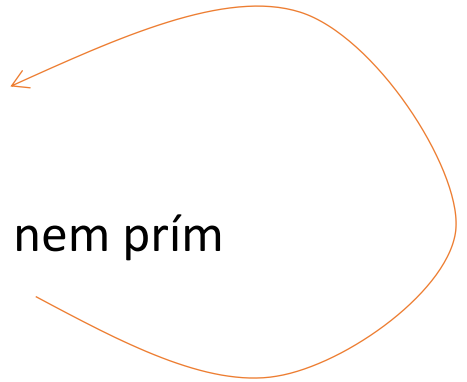


RSA

Lépés	Aliz	Erik	Bob
1			Véletlenszerűen választ két nagy prímszámot, p-t és q-t és kiszámítja az $n = pq$ és $\varphi(n) = (p-1)(q-1)$ értékeket, nyilvános (n, e) kulcsát, és d titkos kulcsát, $1 < e < \varphi(n) = (p-1)(q-1)$ és $\text{lnko}(e, \varphi(n)) = 1$ $1 < d < \varphi(n)$ és $e \cdot d \equiv 1 \bmod \varphi(n)$
2		$\Leftarrow (n, e)$	
3	$c = m^e \bmod n$ szerint rejtjelezi m-et		
4		$c \Rightarrow$	
5			visszafejti c-t $m = c^d \bmod n$ szerint

Prímszámok keresése

- Fermat-tétel
  - p prím és a nem osztható p-vel, akkor
  - $a^{p-1} \equiv 1 \pmod{p}$
- keresés:
  - $a \in [2, p-2]$ véletlen
  - ha nem teljesül a fenti egyenlet, akkor a tanú arra, hogy p nem prím



k-szor

- Carmichael-számok
  - olyan összetett számok, amelyek esetében minden a-ra teljesül a fenti kongruencia

RSA – p és q közeli prímek

- $n = p \cdot q$
  - $p > q$
- legyen
  - $t = \frac{p+q}{s}$ $\qquad p = t + s$
  - $s = \frac{p-q}{2}$ $\qquad q = t - s$
- ekkor
  - $n = t^2 - s^2 = (t + s)(t - s)$
- ha s kicsi, azaz a két prím közel van egymáshoz, akkor
  - $t \approx \sqrt{n}$
  - tippek: $t_1 = \lfloor n^{1/2} \rfloor + 1$, $t_2 = \lfloor n^{1/2} \rfloor + 2$, stb.

RSA - aláírás

Lépés	Aliz	Erik	Bob
1	A következő értékeket választja: $n = pq$, (n, e) nvilvános kulcs és d titkos kulcs		
2		$(n, e) \Rightarrow$	
3	Aláírja az m üzenetet: $\text{sig}_A(m) = m^d \bmod n$		
4		$(m, \text{sig}_A(m)) \Rightarrow$	
5			Ellenőrzi Aliz aláírását $m \equiv (\text{sig}_A(m))^e \bmod n$ segítségével