Óbudai Egyetem

Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar

Műszaki területek informatikai biztonsága

Bevezető, Szimmetrikus kulcsú titkosítások

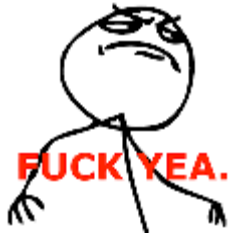
ZENTAI DÁNIEL

ZENTAI.DANIEL@BGK.UNI-OBUDA.HU

233-AS SZOBA

Követelmények

- Utolsó órán zh.
- Órára járni NEM kötelező.



- De aki rendszeresen jár órára (értsd max. 3 alkalommal hiányzik), az kiválthatja a zh-t egy előadás megtartásával a szorgalmi időszakban.
- Az előadásra megajánlott jegyet lehet kapni, ez javítható (vagy rontható) a zh-n.
- A zh anyaga minden, ami az órákon elhangzik, beleértve a hallgatói előadásokat is.

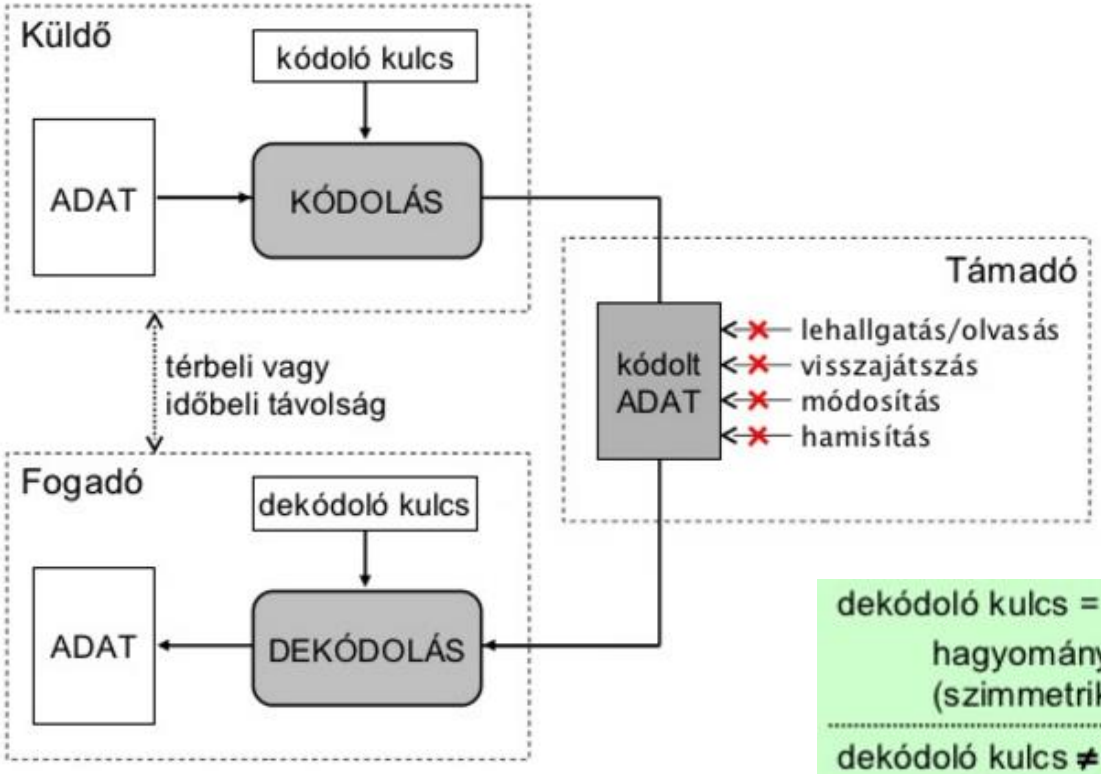
Előadások

- 2013. évi L. törvény
- Enigma
- Elektronikus szavazórendszerek
- Bitcoin
- Jelszótörő programok
- Kvantum kriptográfia
- Cross Site Scripting
- SQL injection
- Egy cikk feldolgozása a eprint.iacr.org oldalról
- Nagyjából bármi…

Miről lesz szó?

- Szimmetrikus kulcsú titkosítás
  - Kulcsfolyam titkosítók
  - Blokktitkosítók
- Aszimmetrikus kulcsú titkosítás
- Kulcscsere protokollok
- Digitális aláírás
- Internet biztonság
- WiFi biztonság
- Nagyjából bármi…

A titkosítás alapmodellje



dekódoló kulcs = kódoló kulcs
hagyományos kriptográfia
(szimmetrikus kulcsú)

dekódoló kulcs ≠ kódoló kulcs
nyílvános kulcsú kriptográfia
(aszimmetrikus kulcsú)

Kerckhoffs elv

Auguste Kerckhoffs, holland kriptográfus (1835-1903)

„A kódolási rendszer megbízhatósága nem függhet a titkosítási algoritmustól, azt csak a kulcs titkának megőrzése garantálja.”

Tehát kerüljük a „security through obscurity” megoldásokat.

Ha maga az algoritmus publikus, azt szélesebb körben lehet tesztelni, és nagyobb valószínűséggel lehet a hibáit kijavítani. Illetve ha a kulcs kompromittálódik, azt sokkal könnyebb cserélni, mintha magát az algoritmust kellene cserélni.

„Történelemóra”

Caesar kód:

A nyílt szöveg minden betűjét helyettesítjük az abc ciklikusan K pozícióval távolabb lévő karakterével. Pl. K = 3:

Nyílt abc: 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

Kód abc: 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

A kulcstér mérete 25.

K = 13-ra külön elnevezést használunk a Caesar kódra: ROT13

A Caesar kód monoalfabetikus, azaz a rejtett szövegben végig ugyanazt a karakterkészletet használjuk.

A monoalfabetikus kódok könnyedén törhetők gyakoriságelemzéssel. A rejtett szöveg n. leggyakoribb karakterét helyettesítjük a nyílt szöveg nyelvének n. leggyakoribb karakterével.

„Történelemóra”

A Caesar kód egy általánosítása:

A K karakterrel való eltolás helyett a kód abc lehet a nyílt abc tetszőleges permutációja. Pl:

Nyílt abc: 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

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

A kulcstér mérete 26!, de a gyakoriságelemzés itt is működik.

„Történelemóra”

Vigenére titkosítás:

Polialfabetikus rejtjelezés

A kulcsszó betűinek megfelelő abc-ből helyettesítünk

	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

Modern kriptográfia

Két fő csoportja van a szimmetrikus kulcsú titkosításoknak. A kulcsfolyam titkosítók a nyílt szöveget bitenként titkosítják, a blokktitkosítók pedig fix méretű blokkokra tördelik a nyílt szöveget, és ezeket a blokkokat titkosítják.

A DES (Data Encryption Standard) egy blokktitkosító, amit az IBM fejlesztett ki a 70-es években Lucifer néven.

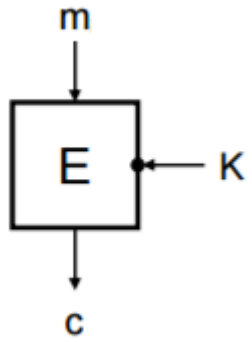
Feistel struktúrára épül (lásd a következő dián).

Modern kriptográfia

Blokktitkosító:

$E:\{0,1\}^s \times \{0,1\}^n \rightarrow \{0,1\}^n$

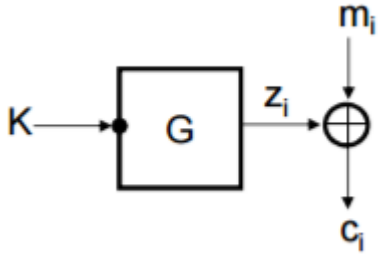
E_K minden fix K esetén invertálható, $E_K^{-1} = D_K$



Kulcsfolyam titkosító:

Bitenként XOR-oljuk a kulcsfolyamot és a nyílt szöveget

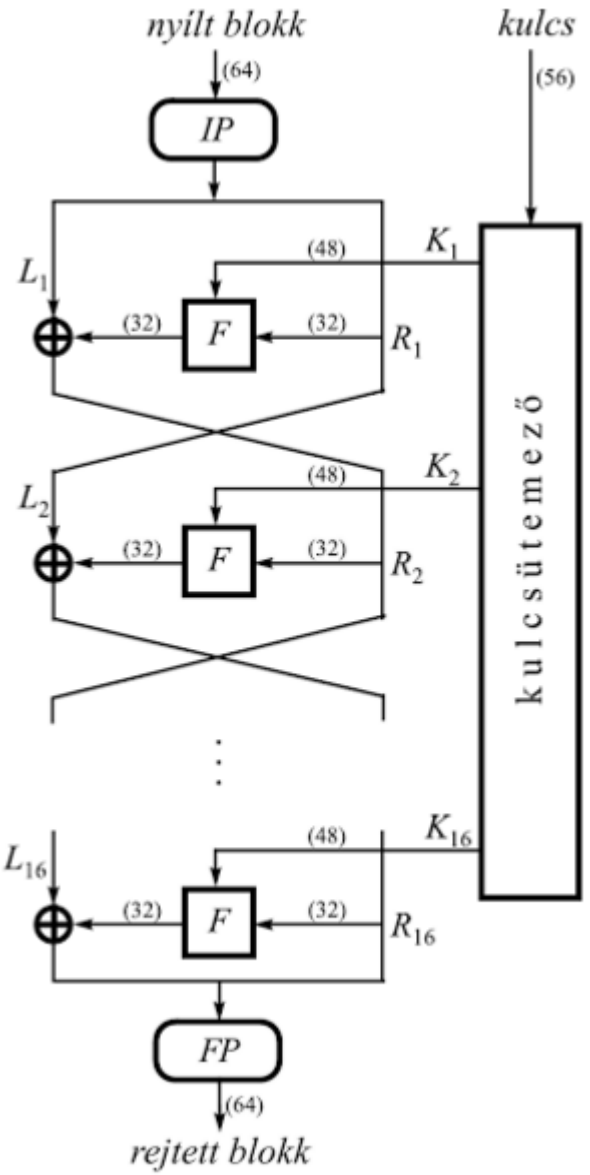
$m = m_1 m_2 \ldots m_n$: nyílt szöveg
$c = c_1 c_2 \ldots c_n$: rejtett szöveg
$K = k_1 k_2 \ldots k_s$: kulcs
E: kódoló transzformáció
D: dekódoló transzformáció
G: kulcsfolyam generátor
$z = z_1 z_2 \ldots z_n$: kulcsfolyam



DES

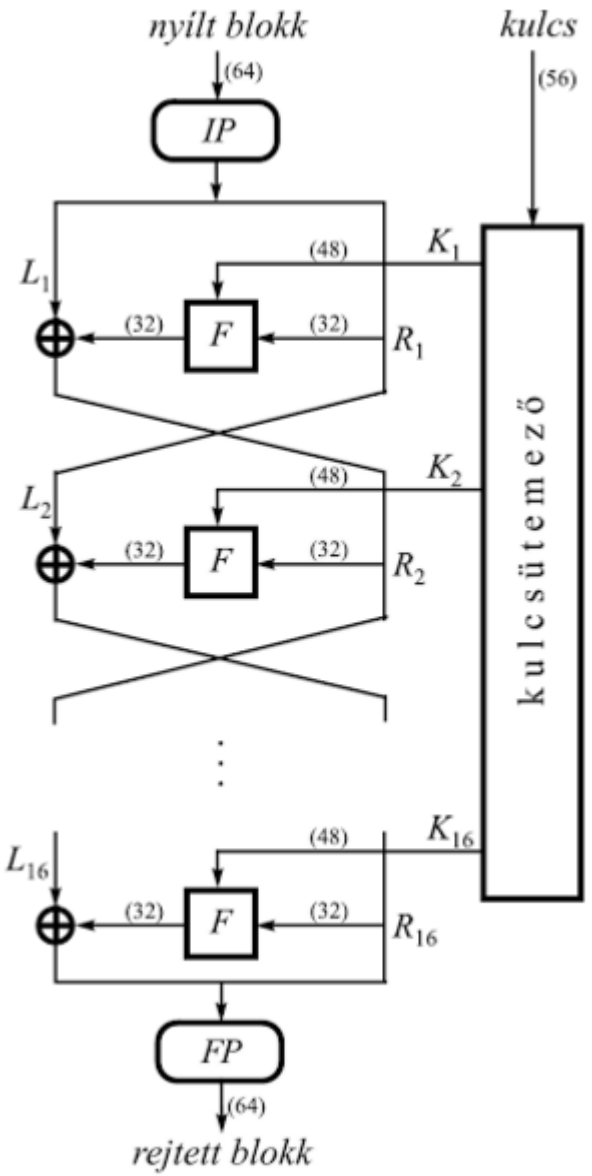
Jellemzői:

- Ma sem ismerünk rá hatékony törést.
- 64 bites input és output
- 16 réteg
- 56 bites kulcs
- Feistel struktúrára épül
- A ma ismert legerősebb támadáshoz is nagyjából 2^{47} nyílt – rejtett szöveg párra van szükség



DES

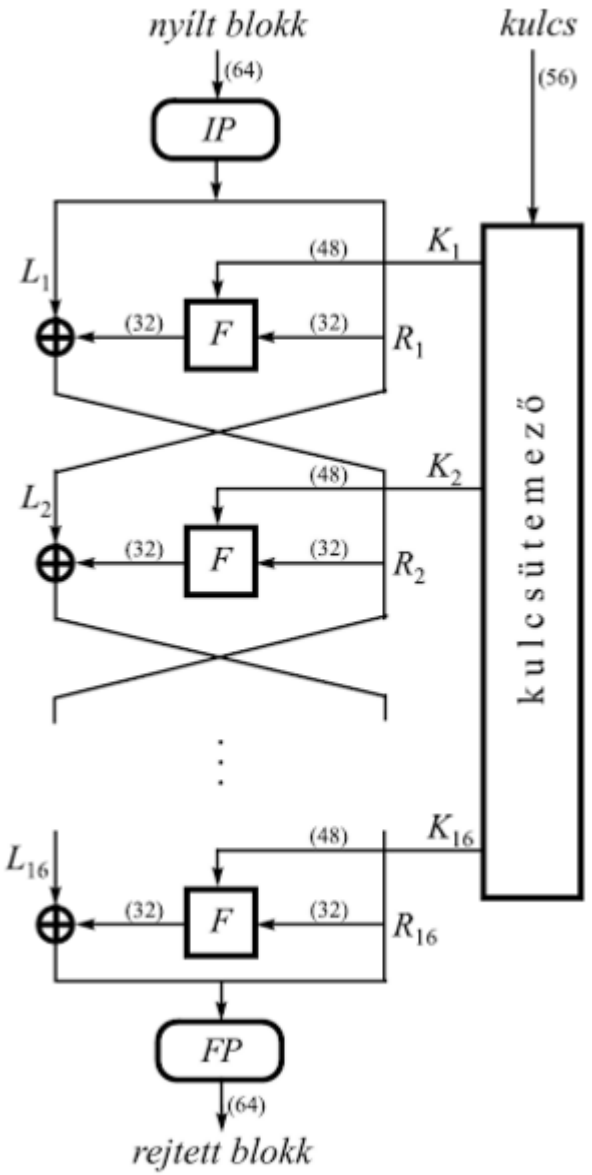
1. A nyílt blokkon alkalmazunk egy IP kezdeti permutációt.
2. Ezt két 32 bites részre vágjuk, ezek lesznek L_1 és R_1.
3. Az i. réteg kulcsát, K_i –t a kulcsütemező állítja elő az 56 bites kulcsból. A rétegkulcsok 48 bitesek.
4. Általános lépésként az F transzformáció kimenetét XOR-oljuk a baloldali blokkal, majd a bal- és jobboldali felcseréljük. Formálisan:
   $L_{i+1} = R_i$
   $R_{i+1} = L_i \oplus F(R_i, K_i)$



DES

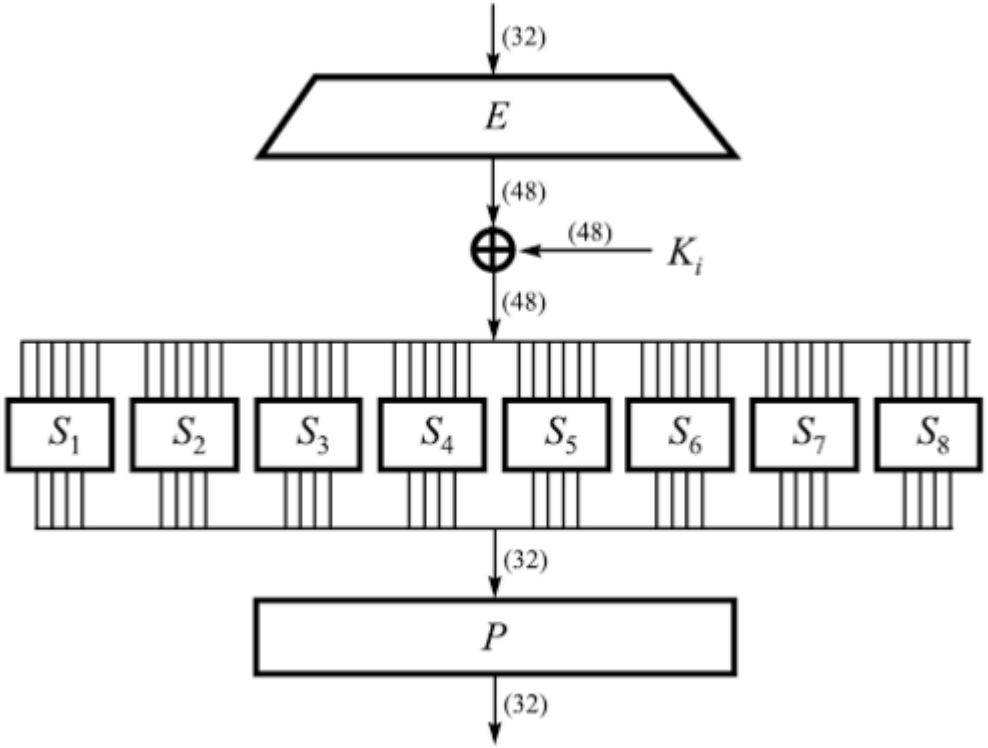
A kulcsütemező:

1. A kulcsütemező állítja elő az egyes rétegek számára a megfelelő kulcsot. Az 56 bites kulcsot két 28 bites részre vágja. Mindkét felét balra rotálja 1 vagy 2 karakterrel (az 1, 2, 9, 16 rétegekben 1-gyel, egyébként 2-vel).
2. Egy a kulcsütemezőbe épített permutáció ebből a 2*28 bitből kiválaszt 48-at, és ezeket használja az F leképezés. A rotálás miatt mindig más bitek kerülnek kiválasztásra a permutációban.



DES

Az F leképezés:



DES

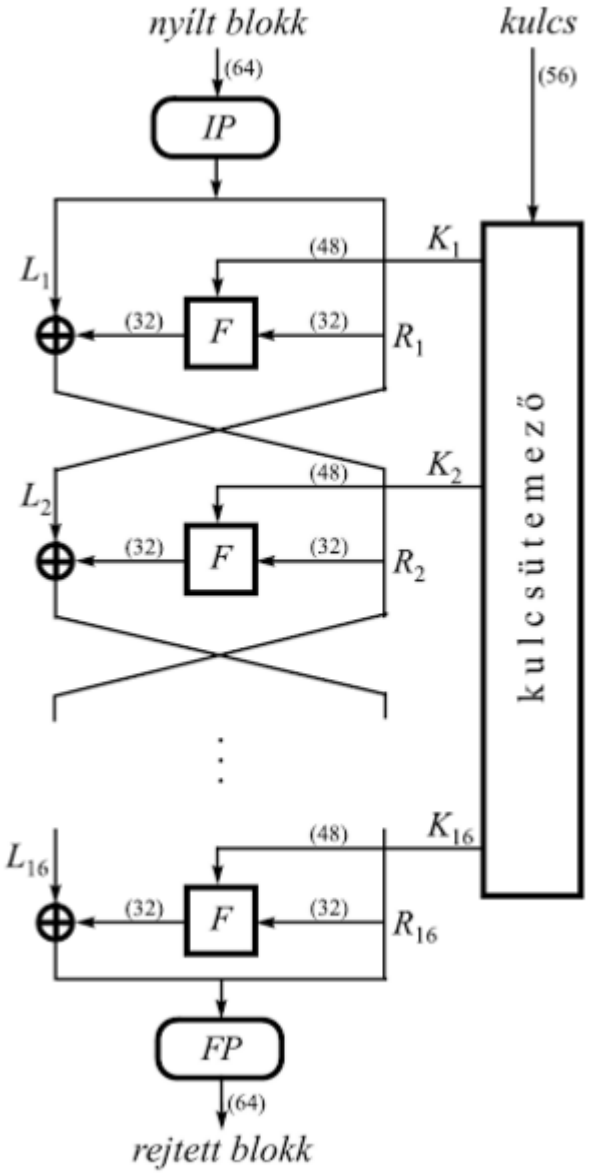
Az F leképezés:

1. Az E expanziós függvény (tulajdonképpen egy visszatevéses permutációa 32 bites inputból generál egy 48 bites stringet, és ezt XOR-olja a K_i rétegkulccsal.
2. Ezt a 48 bitet 8 darab 6 bites blokkra tördeljük, ez lesz az S_i dobozok inputja. Az S_i dobozokban 4 darab 4 bites permutáció található, a 6 input bit két szélső bitje határozza meg, hogy a 4 közül melyik permutációt használjuk.
3. Ezt a 8*4 bitet összefűzzük, és végrehajtunk rajtuk még egy permutációt.

DES

Dekódolás:

1. A permutációk inverzét könnyű kiszámolni.
2. Láttuk, hogy az egyes rétegekre teljesülnek az
   $L_{i+1} = R_i$
   $R_{i+1} = L_i \oplus F(R_i,K_i)$
   összefüggések. Ez alapján
   $R_i = L_{i+1}$
   $L_i = R_{i+1} \oplus F(R_i,K_i)$
3. Fontos, hogy itt az F leképezés inverzét nem kellett kiszámolni, tehát nem is feltétele a dekódolásnak, hogy F invertálható legyen.



3DES

A DES nem minősül biztonságosnak, 1998-ban feltörték 56 óra alatt a Deep Crack nevű (250 000 $ értékű!) számítógéppel. Brute force támadást használtak.

A DES egy lehetséges javítása a 3DES, ami 3 darab DES titkosítás egymás utáni alkalmazását jelenti E-D-E, vagy D-E-D sorrendben. Ez 56 bit helyett 168 bites kulcsméretet garantál.

3DES

Miért nem E-E-E, vagy D-D-D?

Csoport tulajdonságú rejtjelezőknél nem nyerünk semmit az E-E-E, vagy D-D-D sorrenddel.

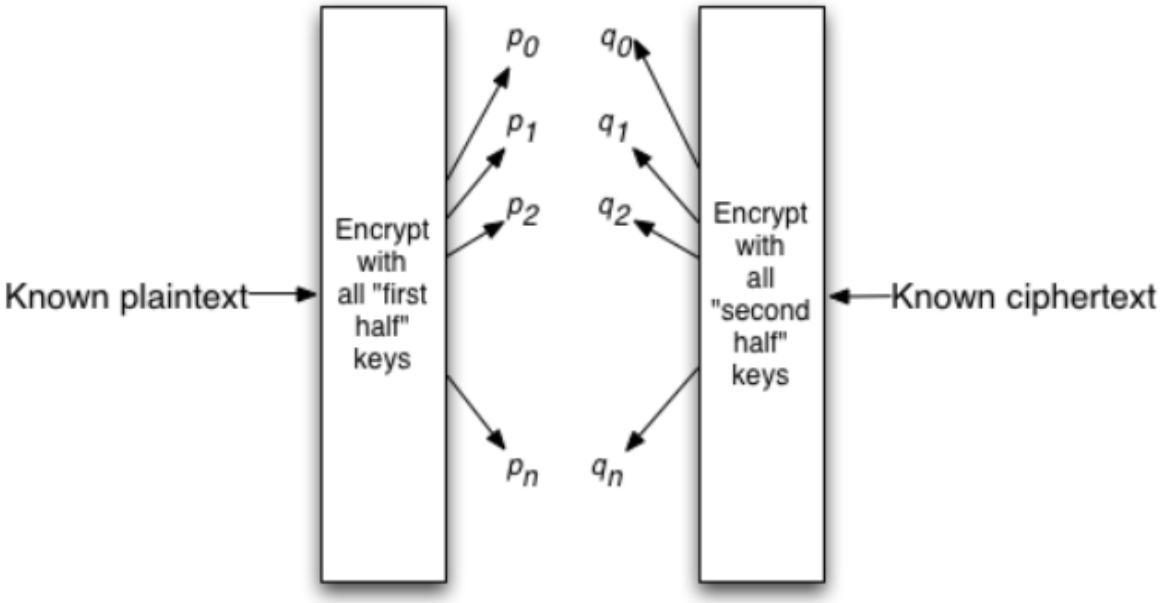
Csoport: (G,*) algebrai struktúra

G zárt a * műveletre
A * művelet asszociatív
G-ben létezik egységelem
G-ben létezik inverz

3DES

Miért nem 2DES?

Meet-in-the-Middle támadással elég $2*2^{56} = 2^{57}$ próbálkozás a kulcs kitalálásához. Tehát csak 1 bitnyi biztonságot nyertünk.



DES-X

A DES egy másik továbbfejlesztése.

K: 56 bites kulcs
K_1, K_2: 64 bites kulcsok
m: üzenet

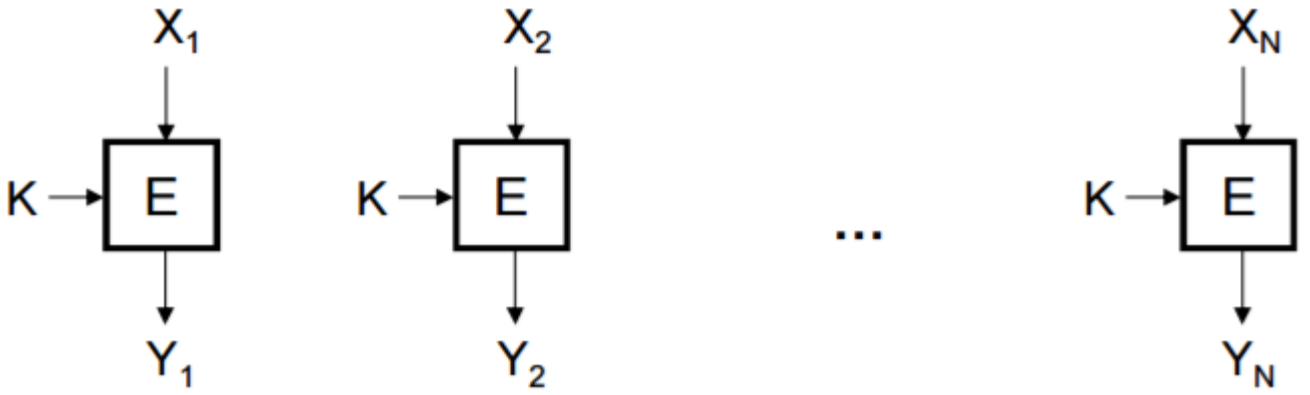
$DESX(m) = K_2 \oplus DES_K(m \oplus K_1)$

A kulcstér mérete: 56+2*64 = 184

Blokktitkosítási módok

Electronic Codebook (ECB) mód

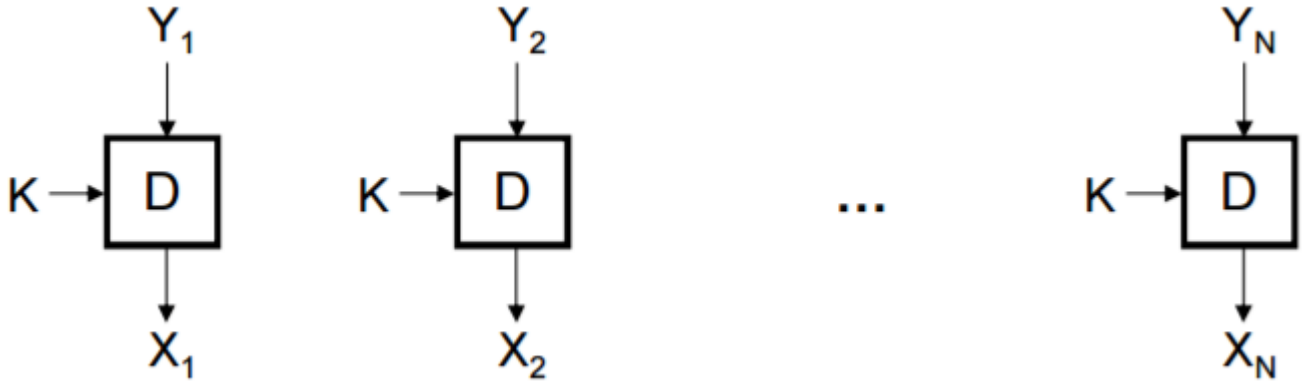
Titkosítás:



Blokktitkosítási módok

Electronic Codebook (ECB) mód

Dekódolás:



Blokktitkosítási módok

Electronic Codebook (ECB) mód

Ugyanazzal a kulccsal titkosítva ugyanazt az üzenetet, a rejtett szöveg is ugyanaz lesz.

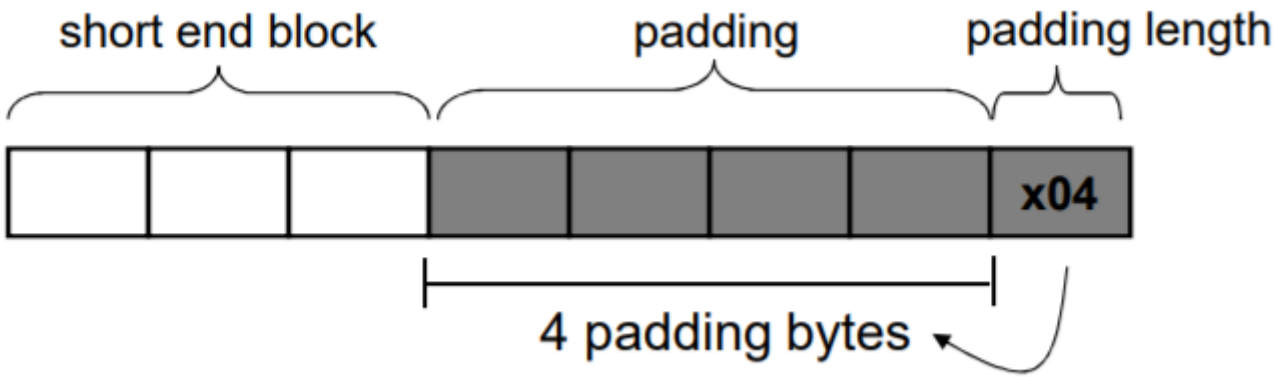
Nem rejti el a nyílt szöveg ismétlődéseit.

A rejtett szöveg blokkok átrendezése nem detektálható. (Szükség van integritás védelemre.)

Egy bit meghibásodása csak az adott blokkot érinti.

Jól párhuzamosítható, de nem ajánlott 1 blokknál nagyobb üzenetekre használni.

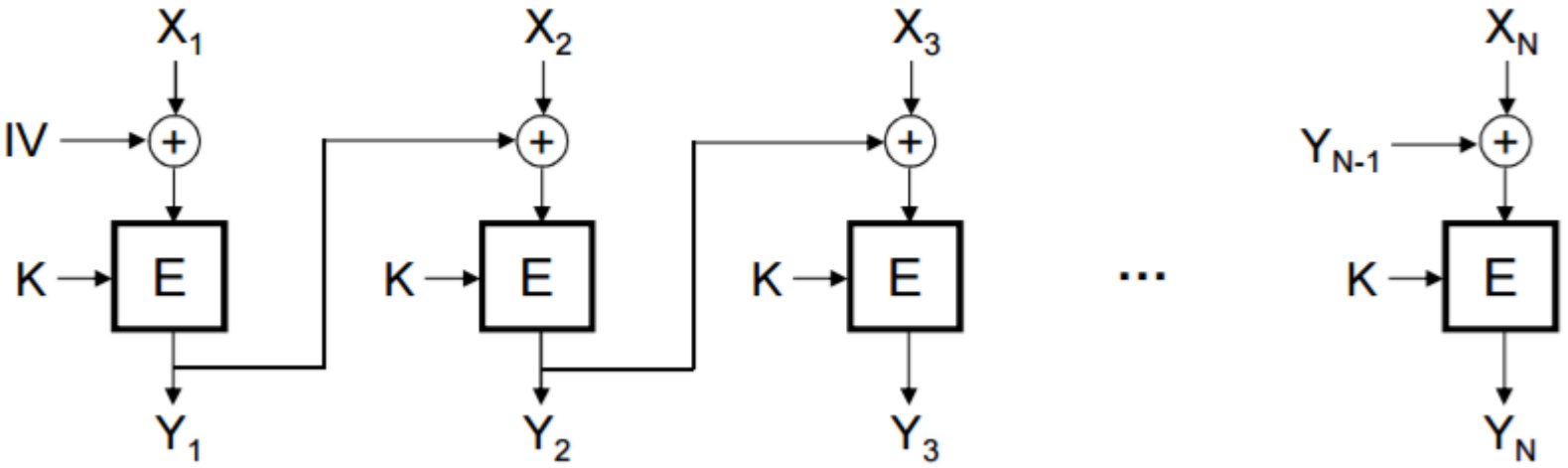
Padding



Blokktitkosítási módok

Cipher Block Chaining (CBC) mód

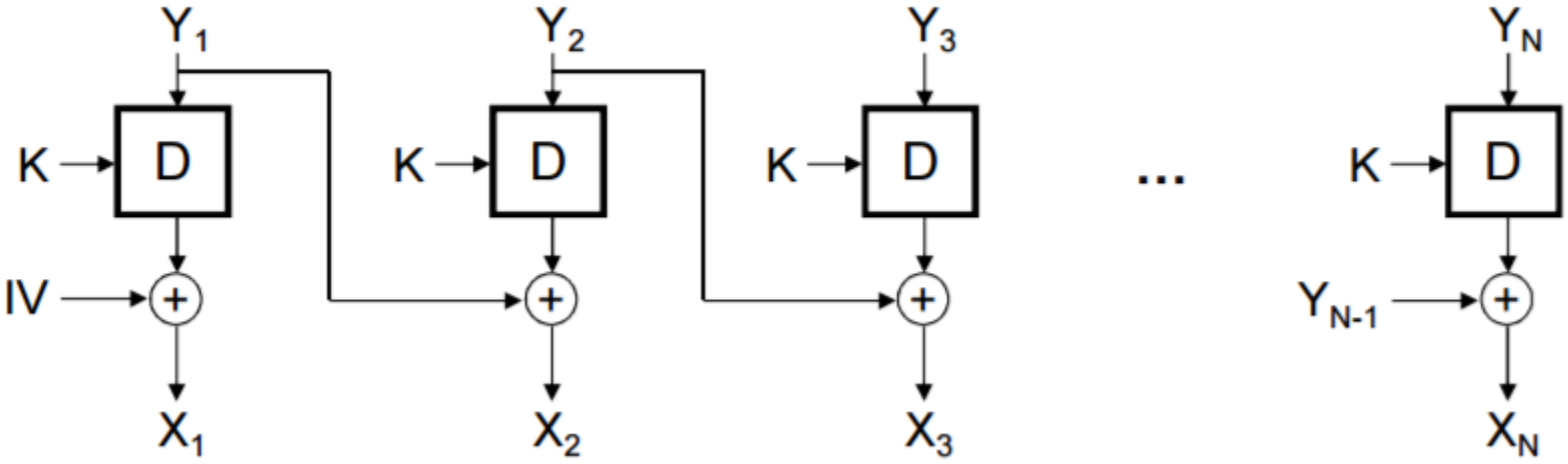
Titkosítás:



Blokktitkosítási módok

Cipher Block Chaining (CBC) mód

Dekódolás:



Blokktitkosítási módok

Cipher Block Chaining (CBC) mód

Különböző IV esetén azonos kulcs, és nyílt szöveg esetén is más lesz a titkos szöveg.

Minden rejtett blokk csak az azonos sorszámú, és az azt követő nyílt blokktól függ, így 1 bit meghibásodása az adott blokkra, és az utána következő blokkra van hatással.

A dekódolás párhuzamosítható.

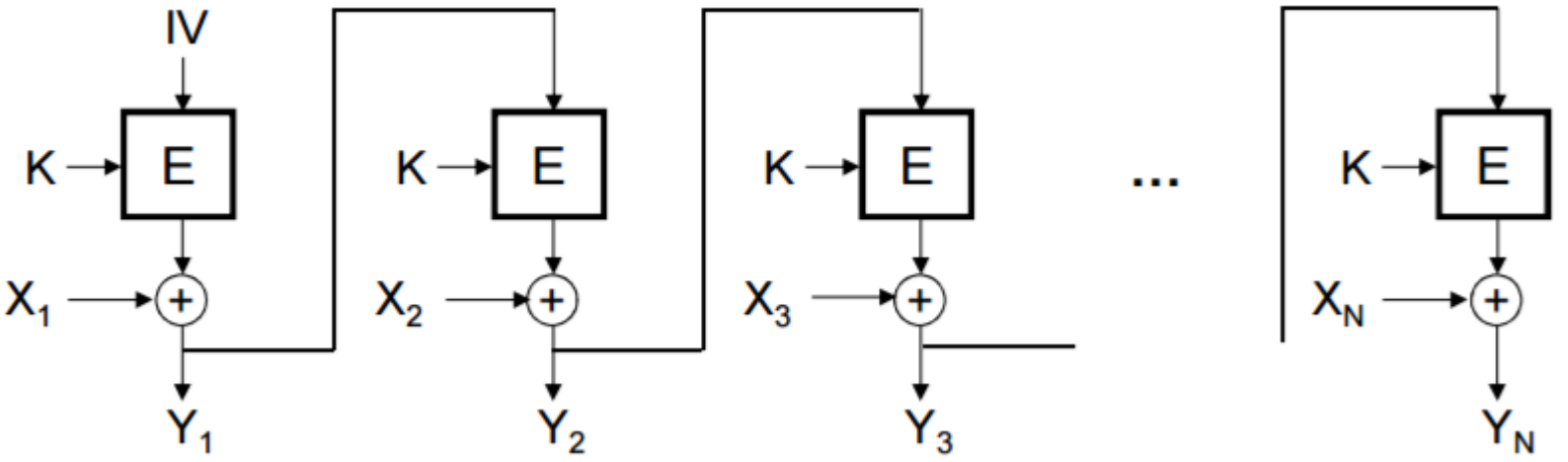
Az IV nem kell hogy titkos legyen, de megjósolhatatlannak kell lennie.

Például IV egy random generátor outputja, vagy IV = $E_K(N)$, ahol N egy nonce.

Blokktitkosítási módok

Cipher Feedback (CFB) mód

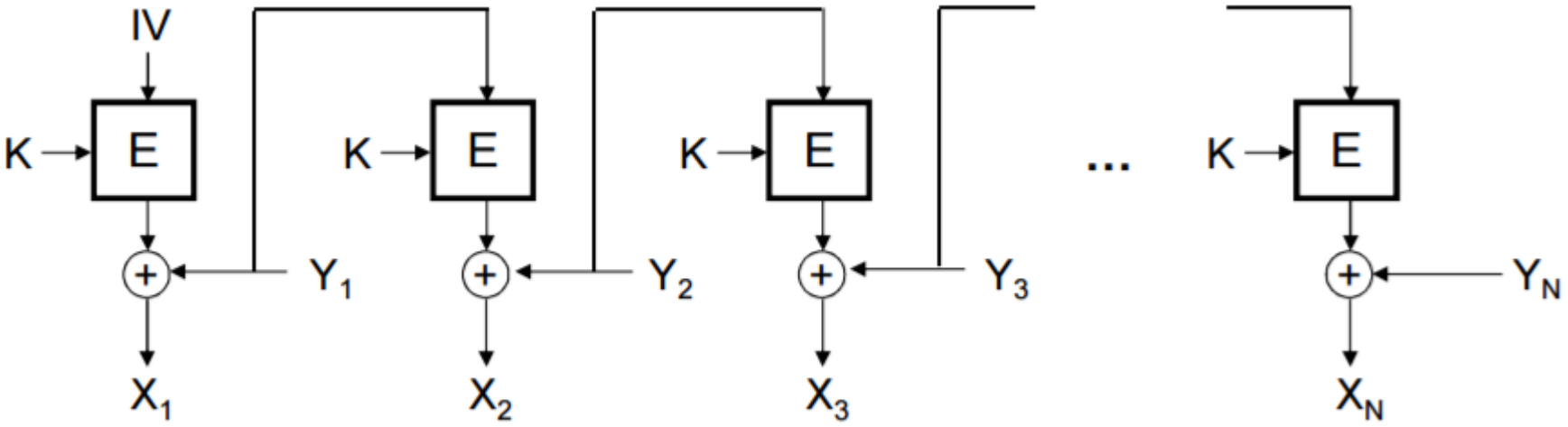
Titkosítás:



Blokktitkosítási módok

Cipher Feedback (CFB) mód

Dekódolás:



Blokktitkosítási módok

Cipher Feedback (CFB) mód

Különböző IV esetén azonos kulcs, és nyílt szöveg esetén is más lesz a titkos szöveg.

Minden rejtett blokk csak az azonos sorszámú, és az azt követő nyílt blokktól függ, így 1 bit meghibásodása az adott blokkra, és az utána következő blokkra van hatással.

A dekódolás párhuzamosítható.

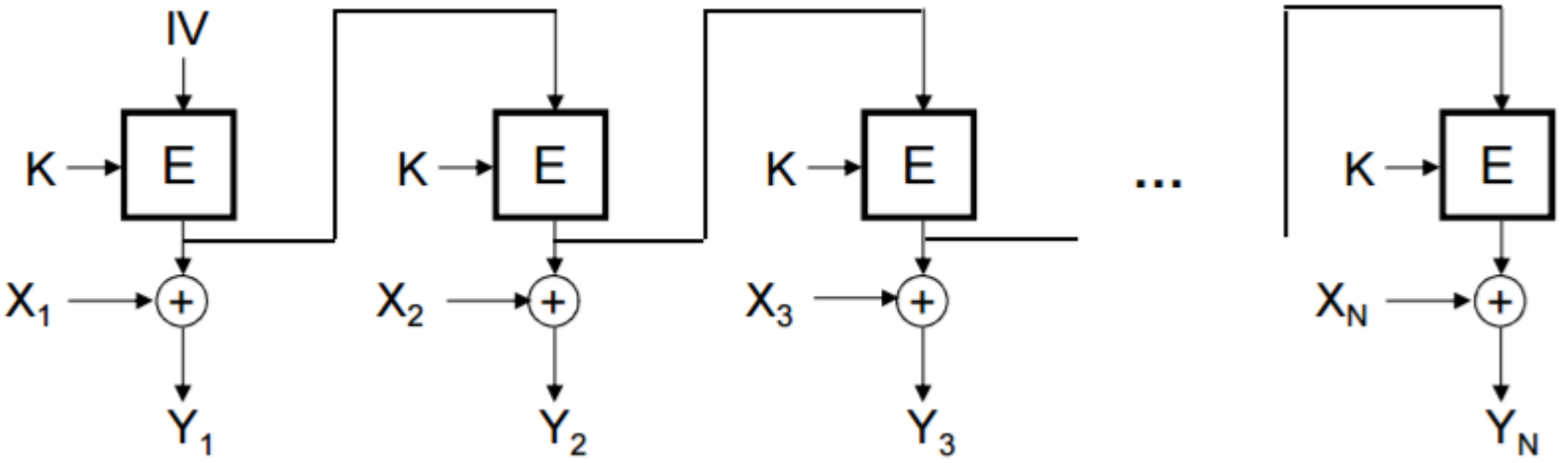
Az IV nem kell hogy titkos legyen, de megjósolhatatlannak kell lennie.

Például IV egy random generátor outputja, vagy IV = $E_K(N)$, ahol N egy nonce.

Blokktitkosítási módok

Output Feedback (OFB) mód

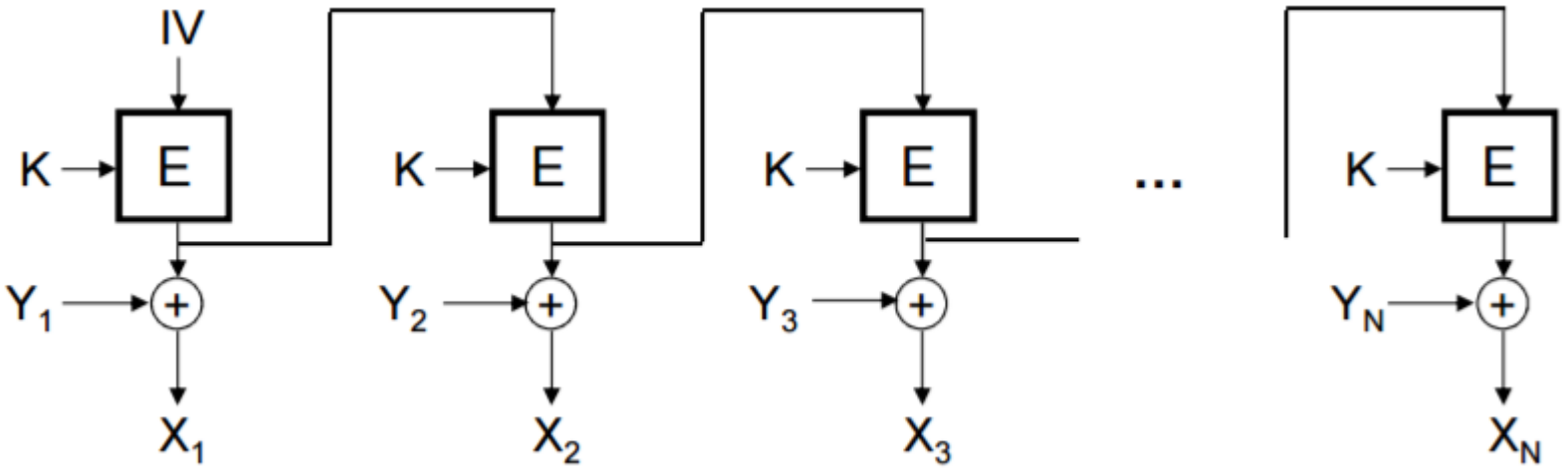
Titkosítás:



Blokktitkosítási módok

Output Feedback (OFB) mód

Dekódolás:



Blokktitkosítási módok

Output Feedback (OFB) mód

Minden üzenet esetén új IV-t kell használni.

Minden rejtett blokk csak az azonos sorszámú nyílt blokktól függ, így 1 bit meghibásodása az adott nyílt blokkra van hatással.

Nem párhuzamosítható.

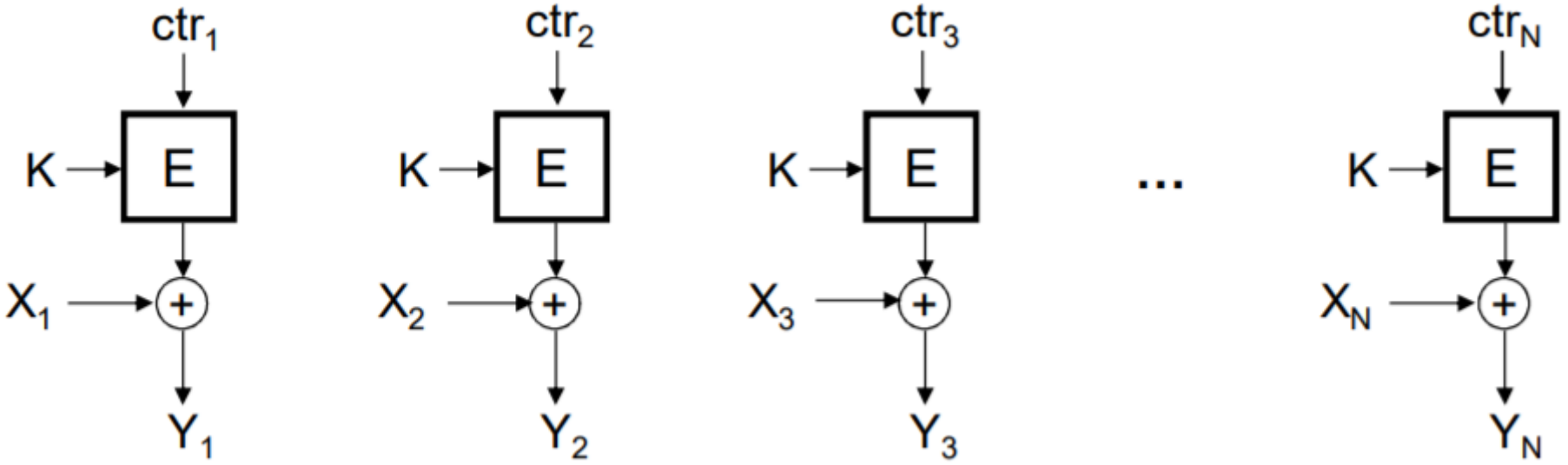
Az IV titkos kell, hogy legyen, és megjósolhatatlannak kell lennie.

Például IV egy random generátor outputja, vagy IV = $E_K(N)$, ahol N egy nonce.

Blokktitkosítási módok

Counter (CTR) mód

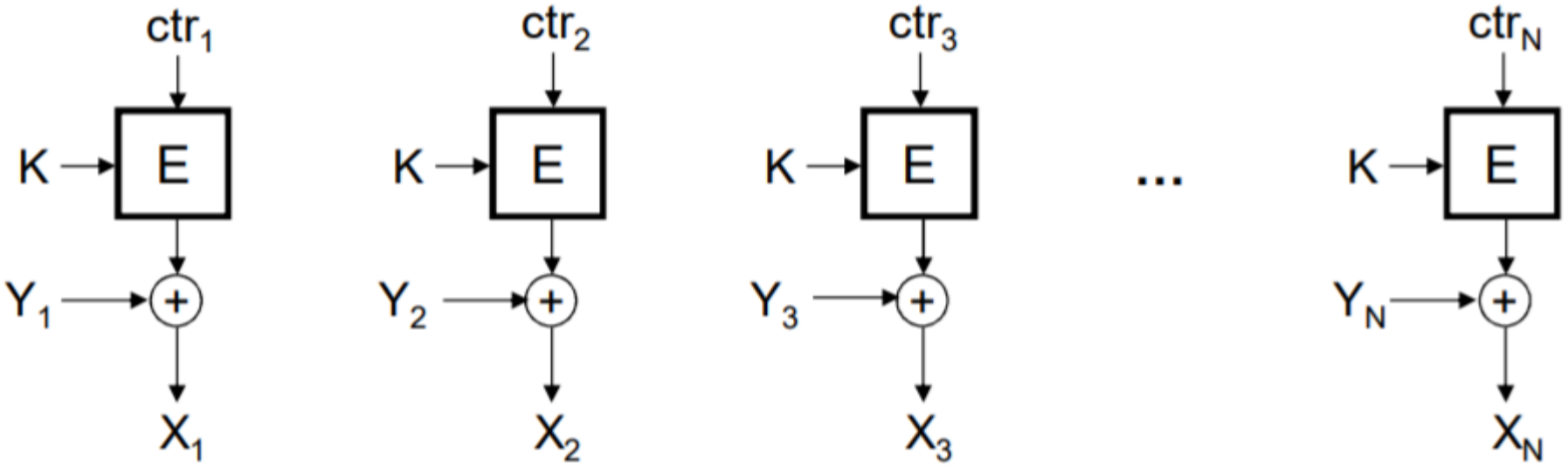
Titkosítás:



Blokktitkosítási módok

Counter (CTR) mód

Dekódolás:



Blokktitkosítási módok

Counter (CTR) mód

Minden rejtett blokk csak az azonos sorszámú nyílt blokktól függ, így 1 bit meghibásodása az adott nyílt blokkra van hatással.

A kódolás és a dekódolás is párhuzamosítható.

Köszönöm a figyelmet!