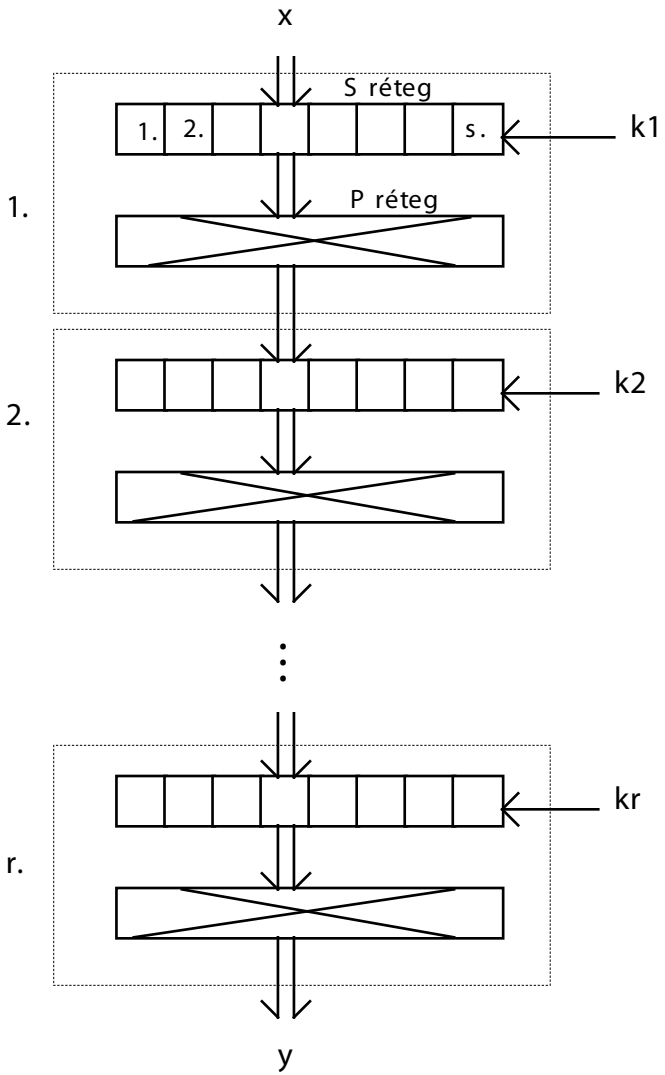
Data Security: Secret key

SPC (Substitution Permutation Cipher)(Tk.2.fejezet bevezető)

Shannon-i elv: *Erős invertálható transzformáció előállítható egyszerű, könnyen analizálható és implementálható, de önmagában gyenge transzformációk sokszori egymás utáni alkalmazásával.*

Példa: szimmetrikus kulcsú rejtjelezők (pl. DES, IDEA, AES)



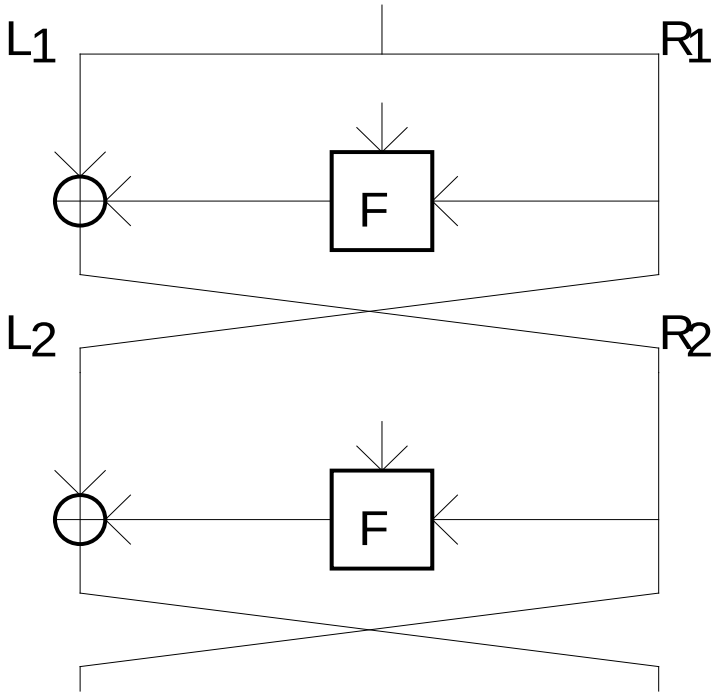
Data Security: Secret key

SPC (DES/Feistel-ötlet) (Tk. 2.1. fejezet)

$L_{i+1} = R_i$
$R_{i+1} = L_i + F(R_i, K_i)$

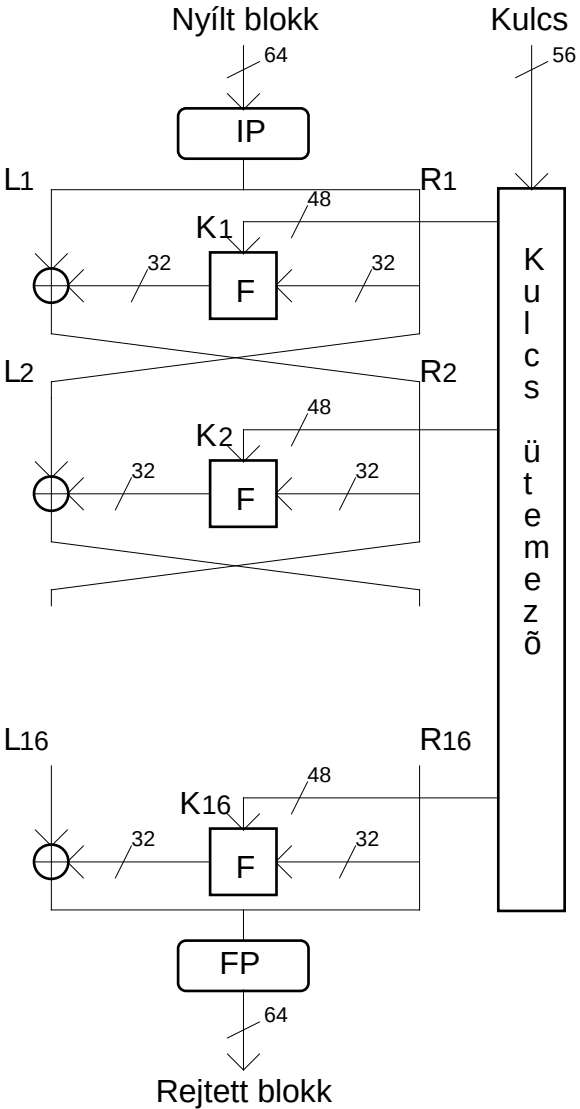
Invertálható, függetlenül attól, hogy *F* invertálható, vagy sem!

$L_i = R_{i+1} + F(L_{i+1}, K_i)$
$R_i = L_{i+1}$



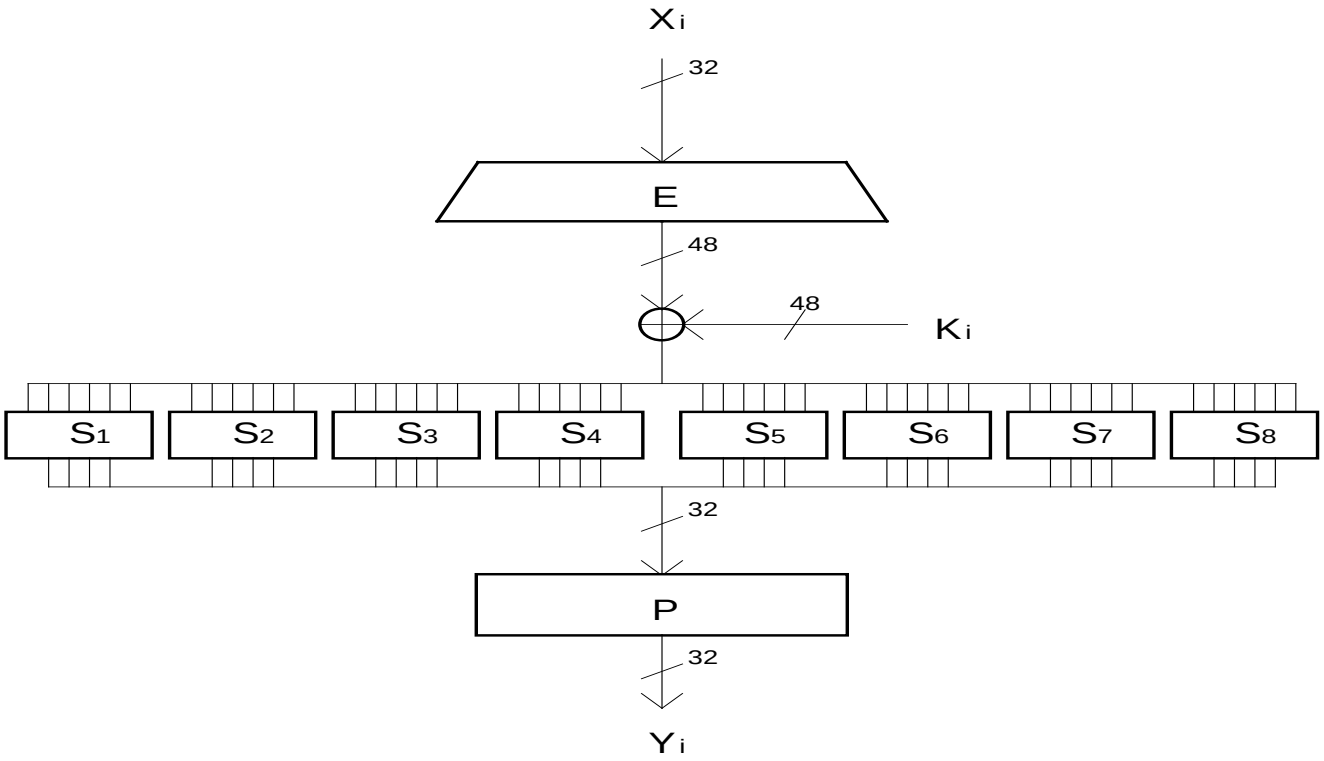
Data Security: Secret key

SPC (DES)



Data Security: Secret key

SPC (DES)



S1 box

14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
4	1	14	8	13	6	2	11	5	12	9	7	3	10	5	0
15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

Data Security: Secret key

Tegyük fel, hogy DES rejtjelezést használunk 64 bites üzenetblokkon és belül a blokk végén 4 bites hibadetekciós ellenőrzőösszeget alkalmazunk.
Egy támadó már megismerte a kulcs első két bitjét, ezután kimerítő kulcskereséses támadást végez. 13 rejtjeles blokk megfigyelése elegendő-e a támadó számára a gyakorlatilag egyértelmű kulcsazonosításhoz?
(Tekintsük gyakorlatilag egyértelműnek a kulcsazonosítást, ha végül csak néhány kulcs közül kell a támadónak választania!)

Igen:
Annak a valószínűsége, hogy téves kulccsal helyes paritásúra dekódolunk egy rejtett szöveg blokkot, 2^{-4} .

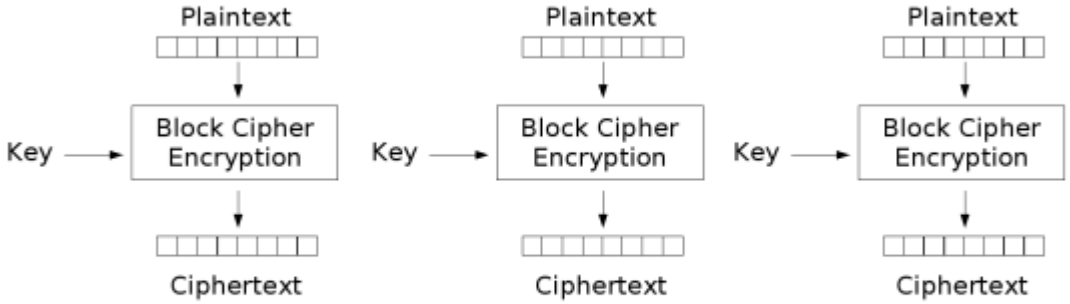
Annak a valószínűsége, hogy 13 rejtjeles blokk mindegyikét helyes paritásúra dekódoljuk téves kulcs mellett $(2^{-4})^{13}=2^{-52}$.

Mivel a kulcstér mérete az előzetesen kiszivárgott két kulcsbit miatt már csak 2^{54}, a nem kiszűrt téves kulcsok átlagos száma a kulcstér teljes végigkeresése után $2^{54}2^{-52} = 2^2 = 4$ lenne.

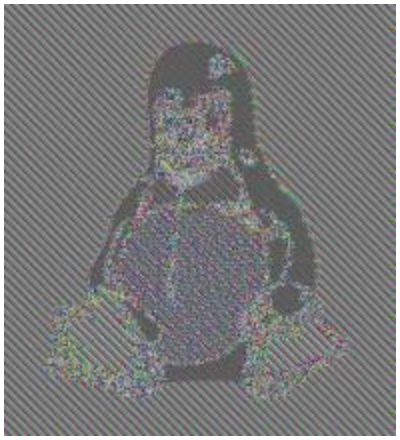
(Tk.2.11.feladat)

Data Security: Secret key

Blokk rejtjelezési módok: ECB (Tk.5.fejezet)

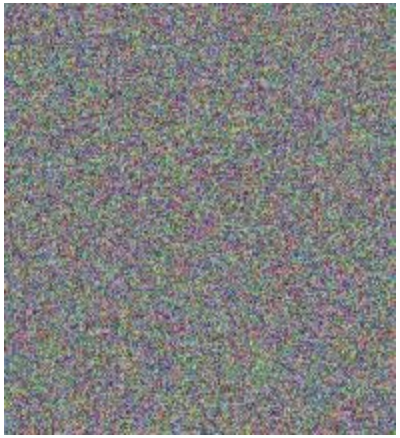


Electronic Codebook (ECB) mode encryption



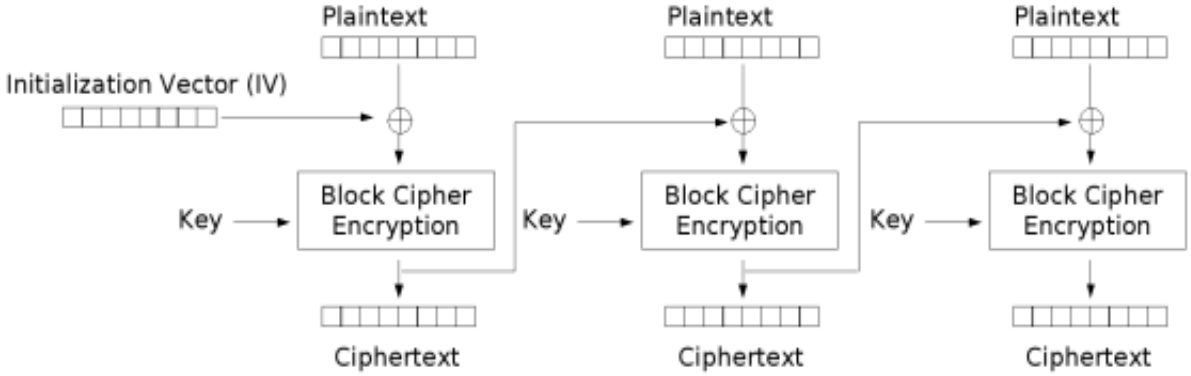
biztonság:

- a nyílt szöveg mintáit nem rejti megfelelően
- a blokkrejtjelező bemenete nem randomizált
- szótár (kódkönyv) alapú támadás lehetséges
- a rejtjeles blokkok felcserélhetők, törölhetők, helyettesíthetők



Data Security: Secret key

Blokk rejtjelezési módok: CBC



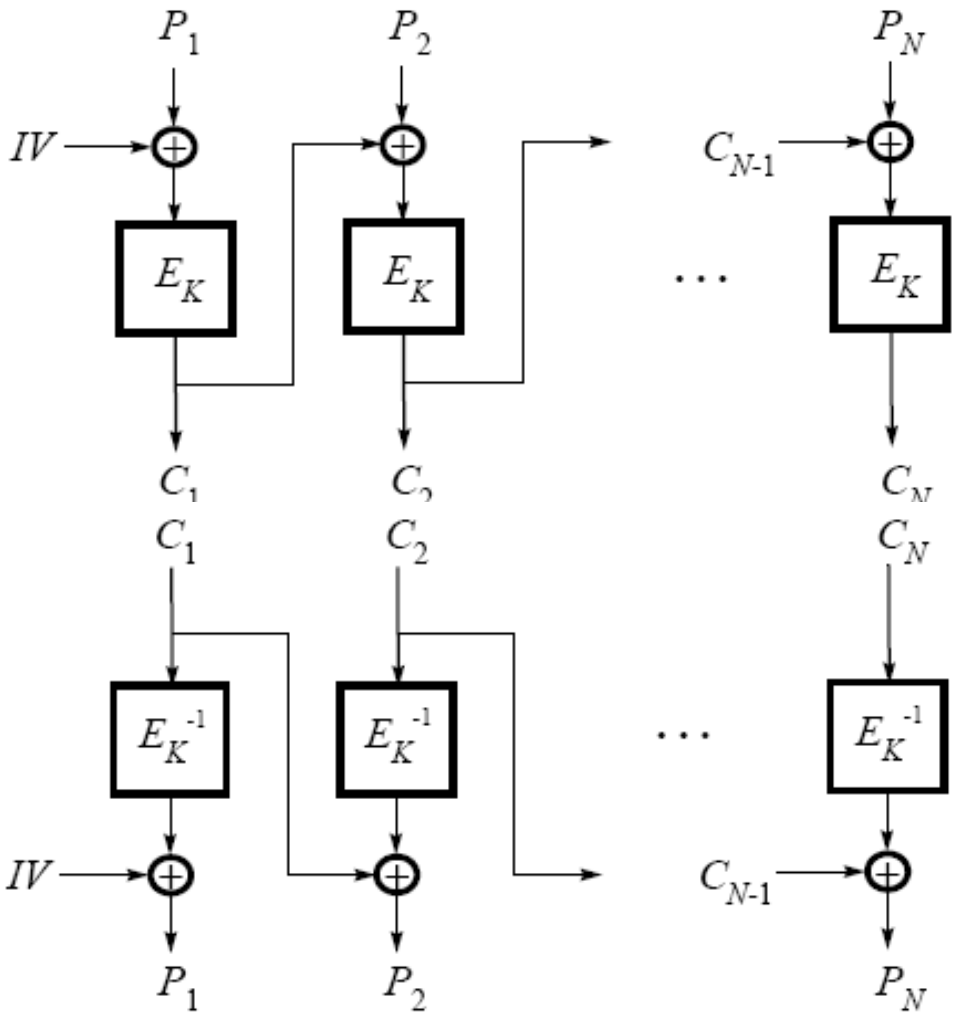
Cipher Block Chaining (CBC) mode encryption

biztonság:

+ a nyílt szöveg mintáit rejti az előző rejtjeles blokkal való XOR-olás
+ a blokkrejtjelező bemenetét randomizálja az előző rejtjeles blokkal való XOR-olás
+ azonos nyílt szövegeket különböző IV-vel rejtjelezve különböző rejtjeles szövegeket kapunk
+ korlátozott mértékben detektálni lehet a rejtjeles blokkok felcserélését, törlését, helyettesítését
– kivág-és-beszúr támadások lehetségesek
– azonos rejtjeles blokkokhoz tartozó nyílt blokkok XOR összegét felfedi

Data Security: Secret key

Blokk rejtjelezési módok: CBC



Data Security: Secret key

Blokk rejtjelezési módok: CBC

128 bites nyílt szöveg blokkok sorozatát AES rejtjelezővel CBC módban rejtjelezzük:
Mennyi blokkot kell rejtjelezni ahhoz, hogy >0.5 valószínűséggel előforduljon két azonos rejtett szöveg blokk?

128 bites rejtett szöveg blokkok összes száma $m=2^{128}$. CBC módban a rejtett szöveg blokkokat modellezhetjük véletlenül választottaknak függetlenül a nyílt szöveg tulajdonságoktól. Így a születésnapi paradoxon alapján $p \sim 1-\exp(-r^2/2m)$ összefüggésből, $p=0.5$ esetén $1.17 \cdot 2^{64}$ eredmény adódik.

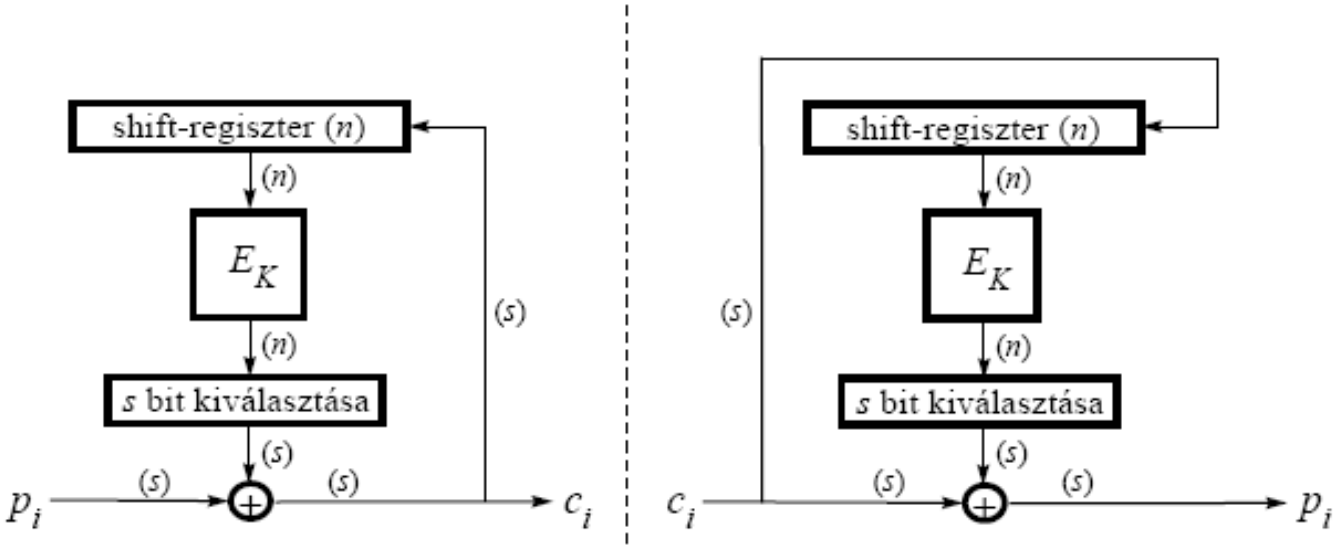
Ha két azonos rejtett szöveg blokkot detektáltunk, mit tudunk mondani a hozzájuk tartozó nyílt szöveg blokkról?

Meg tudjuk határozni a két nyílt szöveg differenciáját!

$$x_k \oplus y_{k-1} = x_i \oplus y_{i-1} \quad \rightarrow \quad x_k \oplus x_i = y_{k-1} \oplus y_{i-1}$$

Data Security: Secret key

Blokk rejtjelezési módok: CFB

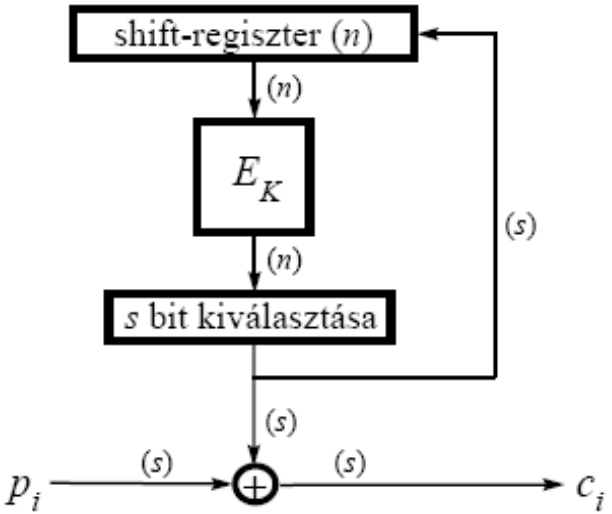


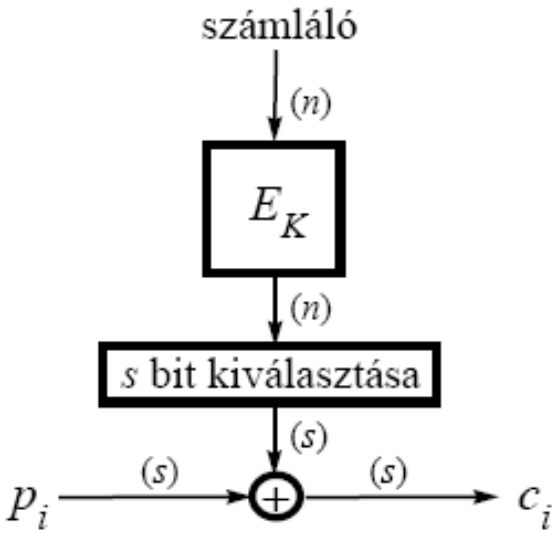
biztonság:

- \+ a nyílt szöveg mintáit rejti
- \+ a blokkrejtjelező bemente véletlen
- \+ azonos nyílt szövegeket különböző IV-vel rejtjelezve különböző rejtjeles szövegeket kapunk
- \+ korlátozott mértékben detektálni lehet a rejtjeles karakterek felcserélését, törlését, helyettesítését
- – utolsó karakter bitjei manipulálhatók

Data Security: Secret key

Blokk rejtjelezési módok: OFB , CTR





biztonság:

+	a nyílt szöveg mintáit rejti
+	azonos nyílt szövegeket különböző IV-vel rejtjelezve különböző rejtjeles szövegeket kapunk
–	különböző nyílt szövegeket azonos IV-vel rejtjelezve a nyílt szövegek megfejthetőek
+/–	korlátozott mértékben detektálni lehet a rejtjeles karakterek felcserélését, törlését, helyettesítését, de nem olyan mértékben, mint CFB mód esetén (a korlátozott hibaterjedés miatt)
–	OFB módban *n*-nél kevesebb bites visszacsatolás esetén a generátor periódushossza jelentősen csökken
+	CTR módban a generátor periódushossza a számláló méretétől függ
–	a visszaállított nyílt karakterek bitjei manipulálhatók

Data Security: Secret key

Blokk rejtjelezési módok: OFB

Véletlen bithibázású csatornán rejtjelezetten továbbítjuk az üzenetünket CBC blokk rejtjelező módban. A véletlen hibázás ellen hibajavító kódolást alkalmazunk. Végezzük a hibajavító kódolást a rejtjelezést megelőzően:

forrás → hibajavító kódolás → rejtjelezés,

rejtjelfejtés → hibajavító dekódolás → nyelő.

a.) Helyesen járunk-e el a fenti módon a hibák javításával kapcsolatosan?

b.) Mi a válasz a kérdésre, ha CBC mód helyett OFB módban rejtjelezünk?

a.) Nem.
A CBC mód hibaterjedés tulajdonsága szerint egy véletlen hiba esetén, hibázás utáni első blokk bitjeinek átlagosan fele hibás lesz, s még a rákövetkező blokk egy bitje. Ezt a nagymértékű meghibásodást csak igen költséges, komplex javító kóddal tudnánk eliminálni. A helyes megoldás a rejtjelezés utáni hibajavító kódolás alkalmazása.

b.) Igen.
Nincs hibaterjedés a kulcsfolyamatos típusú rejtjelezés mód miatt. Ez esetben alkalmazhatjuk a hibajavítást a rejtjelezést megelőzően.

Data Security: Secret key

Blokk rejtjelezési módok

Ha egy csatorna 10^{-9} bithibaaránnyal működik, akkor hogyan alakul a bithibaarány rejtjelezett esetben?

a.)128 bites kódolás ECB rejtjelező módban

b.)128 bites kódolás CBC rejtjelező módban

c.)64 bites kódolás CFB byte alapú folyamrejtjelezésnél

d.)64 bites kódolás OFB byte alapú folyamrejtjelezésnél

a.)	b.)	c.)	d.)
64 E-9	65 E-9	33 E-9	E-9

Data Security: Secret key

Blokk rejtjelezési módok

Javasolható-e RSA blokk kódolás alkalmazása

1.) ECB módban?

2.) OFB módban?

1.) Igen, de csak korlátozottan.

Kulcs küldésre alkalmazható, csak véletlen, illetve nagy információtartalmú üzenet kódolható így. Nyílt szöveg alapú próbálgatás ellen nem véd.

2.) Sohasem alkalmazható.

Az OFB módban az RSA mindkét oldalon kódoló üzemmódban működne, azaz a nyilvános kulcs kellene a dekódoláshoz is.

Data Security: Secret key

Blokk rejtjelezési módok

Melyiket blokk rejtjelező módot **nem** tanácsolná a következő alkalmazási feltételek esetén és miért?

1.) fennáll a kezdővektor (IV) átírásának veszélye

2.) bitkieséses szinkronhibás csatornán továbbítás

3.) nyílt szöveg 3 különböző értéket vehet csak fel

1.) CBC: IV átírással első üzenetblokk támadható

2.) OFB: szinkroncsúszás esetén a kulcsfolyam elcsúszik és véletlen bitfolyamot dekódolunk
vagy CBC: egy bit elvesztése eseten a blokkhatárok az üzenet végéig elcsúsznak

3.) eredeti formában egyiket sem; üzenetteret randomizálással növelni kell

(Tk. 5.1-3 feladatok)