Kriptografi

LYK’15

Tanım

Ana Terimler

- Ciphertext

- Plaintext

Örnek

“Yıldız” verisi şifrelenmelidir. Siz olsanız bu veriyi nasıl şifrelerdiniz. ?

Tanım

Encode

0010010111010111
10 = 975E

Encipher or Encrypt

MO7pExfKrOIARaDVywvNjPIQTrhamS7bxiapY7u/
zarXWval9IL9LJYxtGG8K5WsSha7M75ISle+vDLd
OUFko7CYycPk5o4hvdftIRvL7dlE6VfjTPyua2I1
+zXgEgpBvs0UVNPz4mVsT9J4inwOyU21meAZAdrE
SzBOJM7DDE4ziwt9DtxEU2ptN5acq7q1/f/7aK2p
O+rWxNqWa84rLUidpow5Y30/RPC/QrVYGzx45BGb
VZroruebFHhjWF8Wb1pyBNpavjABp2usX+u1S1ry
+14btd5/OHUjYca6BTJKSR6HJqw==

Decipher or Decrypt

Top Secret Plans

1. Get the money!
2. Get the Guns!
3. Hire the Lawyers!
4. Run for Political Office!!

Base64

Man is distinguished, not only by his reason, but by this singular passion from other animals, which is a lust of the mind, that by a perseverance of delight in the continued and indefatigable generation of knowledge, exceeds the short vehemence of any carnal pleasure.

TWFuIGlzIGRpc3Rpbmd1aXNoZWQsIG5vdCBvbmx5IGJ5IGhpcyByZWFzb24sIGJ1dCBieSB0aGlzIHNpbmd1bGFyIHBhc3Npb24gZnJvbSBvdGhlciBhbmltYWxzLCB3aGljaCBpcyBhIGx1c3Qgb2YgdGhlIG1pbmQsIHRoYXQgYnkgYSBwZXJzZXZlcmFuY2Ugb2YgZGVsaWdodCBpbiB0aGUgY29udGludWVkIGFuZCBpbmRlZmF0aWdhYmxlIGdlbmVyYXRpb24gb2Yga25vd2xlZGdlLCBleGNlZWRzIHRoZSBzaG9ydCB2ZWhlbWVuY2Ugb2YgYW55IGNhcm5hbCBwbGVhc3VyZS4=

Base64

Text content	M								a								n							
ASCII	77 (0x4d)								97 (0x61)								110 (0x6e)							
Bit pattern	0	1	0	0	1	1	0	1	0	1	1	0	0	0	0	1	0	1	1	0	1	1	1	0
Index	19								22				5				46							
Base64-encoded	T								W				F				u							

The Base64 index table:

Value	Char	Value	Char	Value	Char	Value	Char
0	A	16	Q	32	g	48	w
1	B	17	R	33	h	49	x
2	C	18	S	34	i	50	y
3	D	19	T	35	j	51	z
4	E	20	U	36	k	52	0
5	F	21	V	37	l	53	1
6	G	22	W	38	m	54	2
7	H	23	X	39	n	55	3
8	I	24	Y	40	o	56	4
9	J	25	Z	41	p	57	5
10	K	26	a	42	q	58	6
11	L	27	b	43	r	59	7
12	M	28	c	44	s	60	8
13	N	29	d	45	t	61	9
14	O	30	e	46	u	62	+
15	P	31	f	47	v	63	/

Kerckhoff Prensibi

Bir kripto sistemin güvenliği algoritmasını gizli tutmaya bağlı olmamalıdır. Sadece secret key’inin gizli olmasına bağlı olmalıdır.

Exclusive OR (XOR)

Input		Output
0	0	0
0	1	1
1	0	1
1	1	0

XOR

1. Değişme Özelliği

$a \otimes b = b \otimes a$

2. Sıfırlama Özelliği

$a \otimes a = 0$

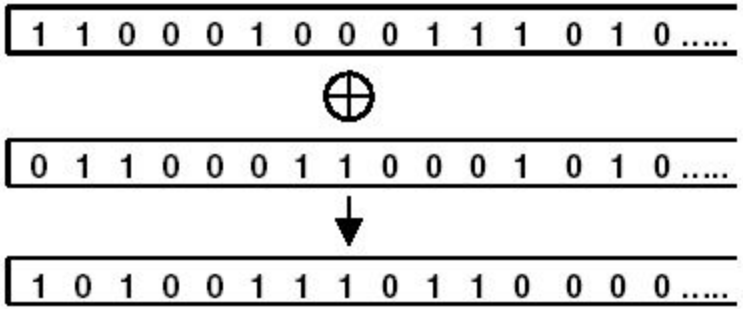
3. Sıfır ile İşlem

$a \otimes 0 = a$

$a \otimes b \otimes a = ?$

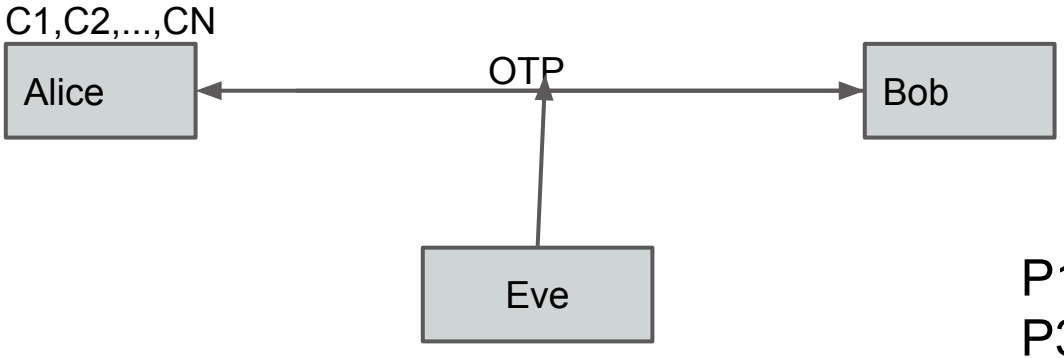
OTP

- Vernam



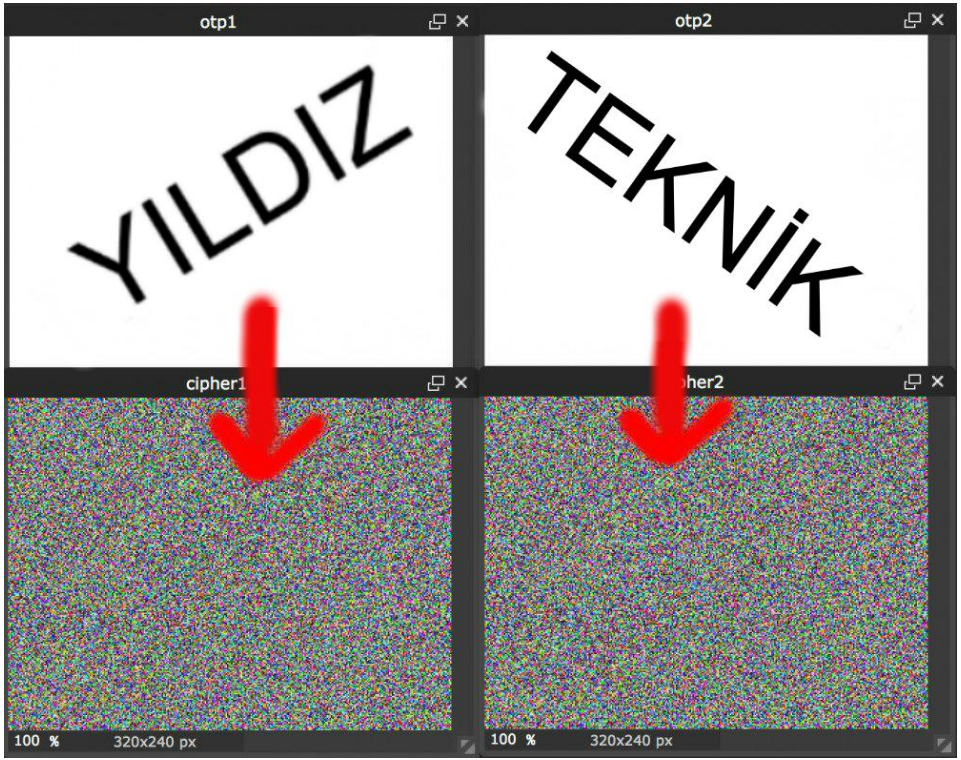
Problem?

OTP

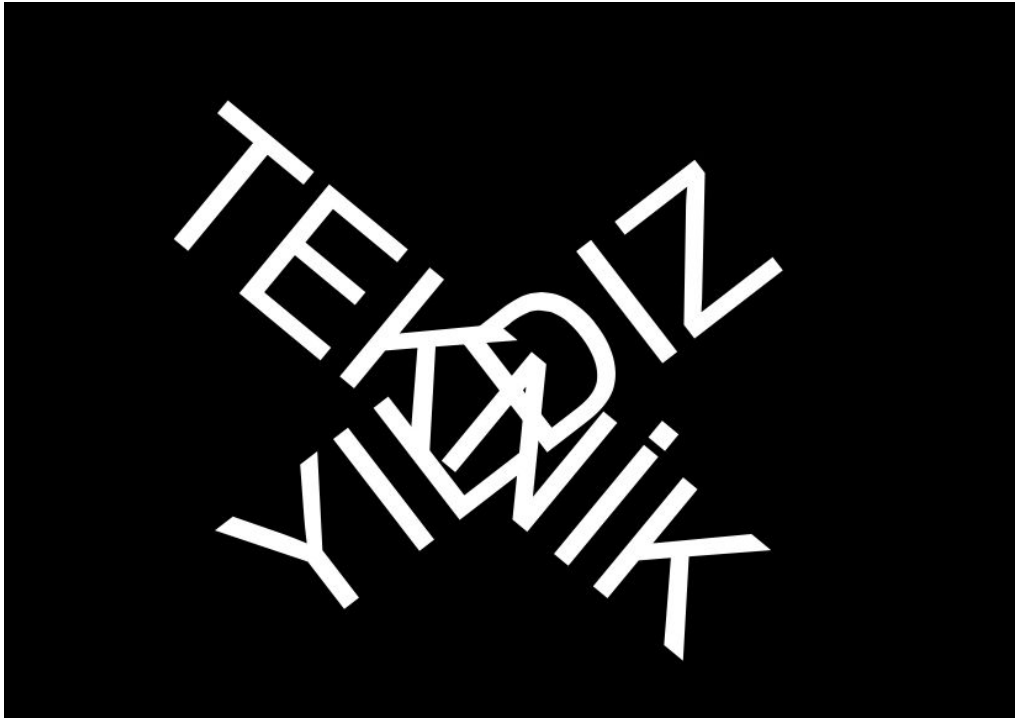


$$P1 \otimes K1 = C1$$
$$P3 \otimes K1 = C3$$
$$P1 \otimes P3 \otimes K1 \otimes K1 = C1 \otimes C3$$

OTP

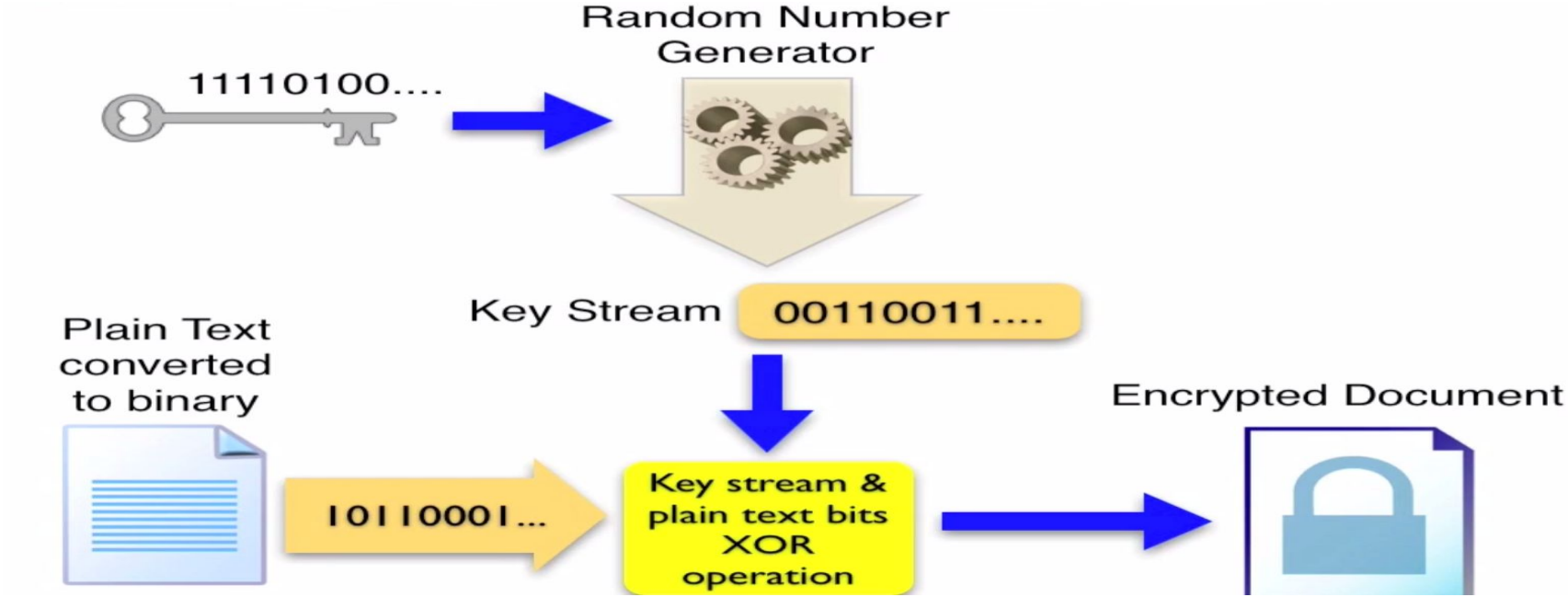

otp1
YILDIZ
otp2
TEKNİK
cipher1
her2
100 %
320x240 px
100 %
320x240 px

OTP



Stream Cipher

❖ Çözüm:



Pseudo Random Number Generator

$$X_{i+1} = (aX_i + c) \bmod M$$

$$X_1 = (5130 + 37) \bmod 100 = (687) \bmod 100 = 87$$ i=0

$$X_2 = (587 + 37) \bmod 100 = (472) \bmod 100 = 72$$ i=1

...

$$X_{n+1} = (5X_n + 37) \bmod 100$$ i=n

Ceaser Cipher (Shift Cipher)

ABCDEFGHIJKLMNOPQRSTUVWXYZ
DEFGHIJKLMNOPQRSTUVWXYZABC

Örnek : Yıldız

Cryptanalysis Ex:

Digraphs in the ciphertext with B

- - QBQ- - - - - - - - - - - - - - - WBU- - - - - - - - - QBN- - YBV- - -

- - - QBO- - - - - - - - - - - - - - - - - - - QBZ- WBO- - - QBKBYYBO - - - - QBH- - - - MBY- - - - - - - - - - - - - - - - - MBP- WBZ- - - - -

- - - UBN- - QBT- - WBR- - QBO- QBTBH- - LBY- - - QBV- PBH- - - - QBT- - - - - - - - - - - - YBYQBG- - - - - KBYYBO- - - QBH-

- - - MBY- - PBK- - - - - - - - - - QBZ- QBO-

The Digraph Frequencies in the English Language

th he an in er on re ed nd ha at en es of nt ea ti to io le is ou ar as de rt ve

Digraph Frequency in the ciphertext with B

BG	BH	BK	BN	BO	BP	BR	BQ	BT	BU	BV	BY	BZ	KB	LB	MB	PB	QB	TB	UB	WB	YB
1	4	1	2	6	1	1	1	3	1	2	6	3	2	1	3	2	15	1	1	4	4

$e_\pi(HE)=QB \Rightarrow e_\pi(H)=Q$ $e_\pi(ER)=BO$ or $BY \Rightarrow e_\pi(R)=O$ or Y

Cryptanalysis Ex:

The Trigraph Frequencies in the English Language

the and tha ent ion tio for nde has nce tis oft men

Trigraphs in the ciphertext such as xQB and Byz

- GQBQH - - - - - - - - - - - - - VWBUY - - - - - - - XQBNOZYBVY - - - - EQBOY - - - - - - - - - - - - - - - - YQBZOWBOZ - YQBKBYYBOT - - YQBHK - - HMBYY - - - - - - - - - - - - - - - WMBPHWBZD - - - - - - ZUBNVTQBTYZWBRVEQBOYQBTBHUWLBYH - YQBVOPBHU - - LQBTQ - - - - - - - - - - - DYBYQBGZ - - - QKBYYBOZ - YQBHK - - HMBYUHPBKX - - - - - - - - YQBZYQBOT

The Trigraph Frequencies in the ciphertext such as xQB and Byz

BGZ	BHK	BHU	BKX	BNO	BNV	BOT	BOY	BOZ	BPH	BRV	BTY
1	2	1	1	1	1	2	1	1	1	1	1

BUY	BVY	BYQ	BYU	BZD	GQB	EQB	LQB	TQB	XQB	YQB
1	1	1	1	1	1	1	1	1	1	6

e_π(THE) = YQB ⇒ e_π(T) = Y ⇒ e_π(R) = O e_π(ENT)=BTY or BUY or BVY⇒e_π(N)=T or U or V

Cryptanalysis Ex:

Digraphs in the ciphertext with Y

- - - - - - - - - XYQ- - - - - - - - - - UYV- KYZ- - - - - - - ZYBVYV- - - - - - OYQHYV- - - - - - - - - - - - LYQ- - - - - - - GYQ- - BYYB- - - GYQ- - - - - - - BYYQHYUZYH- - - - - - - - - - - - - - - - DYV- - - - - - - - - - - - - TYZ- - - - - - - OYQ- - - - - - - BYHYYQ- TYVYDYBYQ- - - - OYQ- BYYB- - GYQ- - - - - - - BYU- - - - - - - - - - - - ZYQ- ZYQ- - -

Digraph Frequency in the ciphertext with Y

BY	DY	HY	GY	KY	OY	TY	UY	VY	XY	YB	YD	YH	YQ	YU	YV	YZ	ZY
4	2	2	1	1	3	2	1	2	1	3	1	1	9	2	4	2	4

eπ(TH) = YQ eπ(ET) = BY eπ(TI or TO) = YV

Cryptanalysis Ex:

Trigraphs in the ciphertext such as Yxy

- - - - - - - - - - YQV- - - - - - - - - - YVH- - - - - - - - - - - YBVYVU - - - - - - YQHYVT- YQHYUZYHN- - - - - - - - - - - - - - - - YVG- - - - - - - - - - - - - YZW- - - - - - - - - - - - - - - - - - YHY- YVYDY- - - - - - - - YQK- - - - - - - - - - - - - - - - - - YUH- -

The Trigraph Frequencies in the ciphertext such as YQx and Yxy

YBV	YDY	YHN	YHY	YQV	YQH	YQK	YUH	YUZ	YVG	YVH	YVT	YVU
1	1	1	1	1	2	1	1	1	1	1	1	1

YVY	YZW
1	1

e_π(THA) = YQH ⇒ e_π(A) = H

e_π(TIO or TIS)=YVG or YVT or YVU⇒e_π(I)=V

Cryptanalysis Example:

Ciphertext:

VGQBQHWHUXYQVULRZUGVWBUYVHKYZTHXQBNOZYBVYVURVEQBO
YQHYVTMXTZRQHULVULYQBZOWBOZGYQBKBYYBOTZGYQBHKEQHM
BYYQHYUZYHNZOWRZDKWMBPHWBZDYVGHUXZUBNVTQBTYZWBRV
EQBOYQBTBHUWLBYHYYQBVOPBHUVULQBTQZDKWTDMTYVYDYBY
QBGZDOYQKBYYBOZGYQBHKEQHMBYUHPBKXGZOHUWTZYQBZYQBO

Letter Frequency in the English Language

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

Letter Frequency in the ciphertext

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

0 13 0 2 1 0 3 7 0 0 3 2 2 1 4 1 9 2 0 4 6 6 4 2 13 7

eπ(E)=B veya Y and eπ(T)=B veya Y

Permutation Cipher

m=6

Encryption: $\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 3 & 1 & 6 & 2 & 5 \end{pmatrix}$

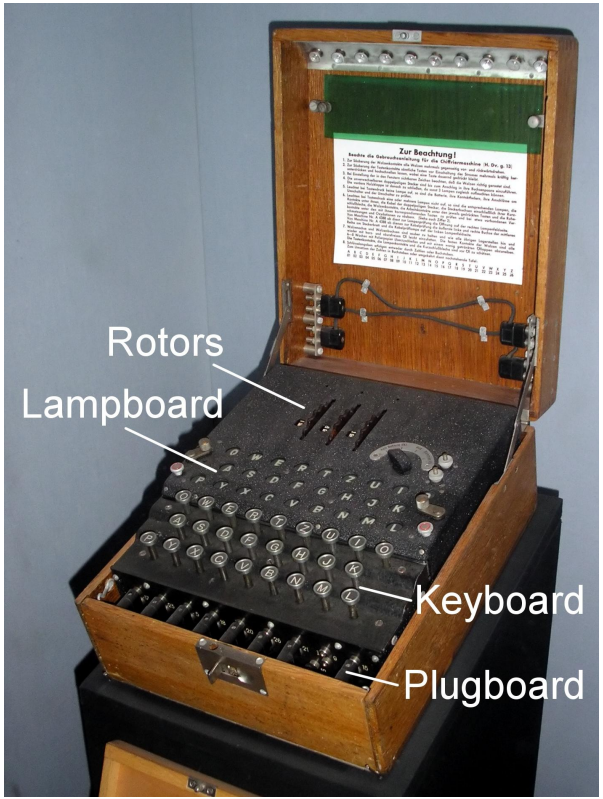
plaintext: he walked up and down the passage two or three times

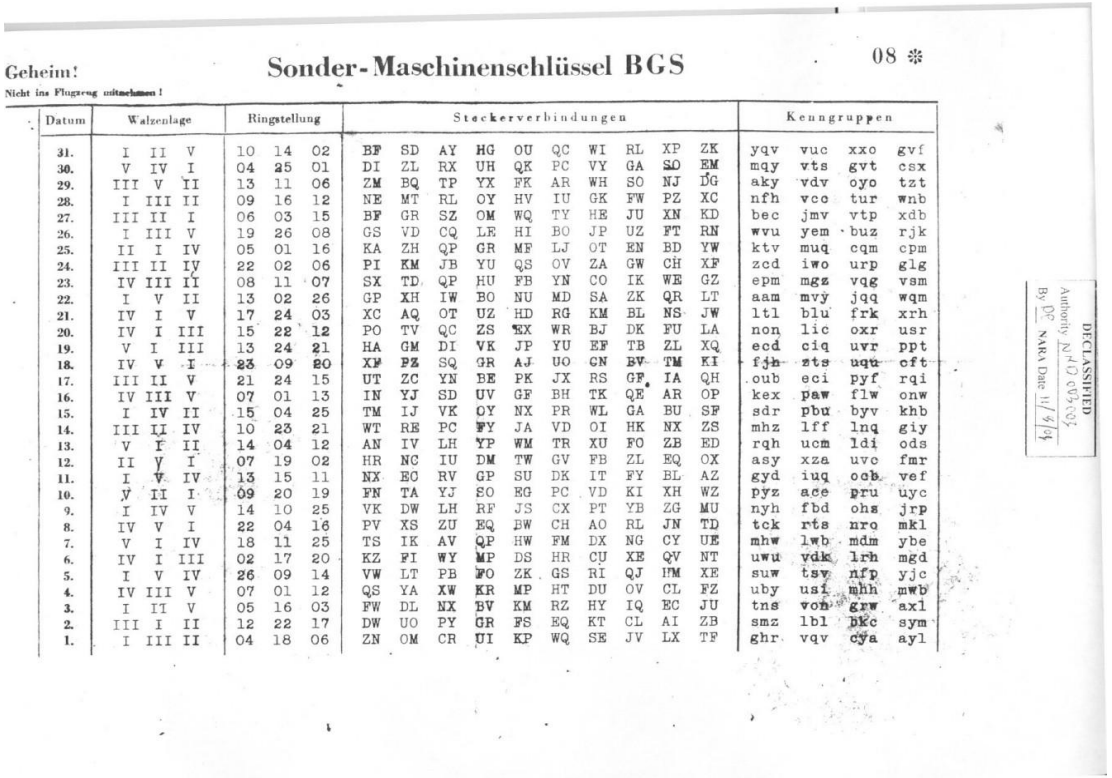
hewalk edupan ddownt hepass agetwo orthre etimes

ciphertext: WLEHKAUADENPONDDTWPSEHSAEWGAOTTRROEHIETESM

Decryption: $\pi^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 5 & 2 & 1 & 6 & 4 \end{pmatrix}$

Enigma Makinası





Geheim!

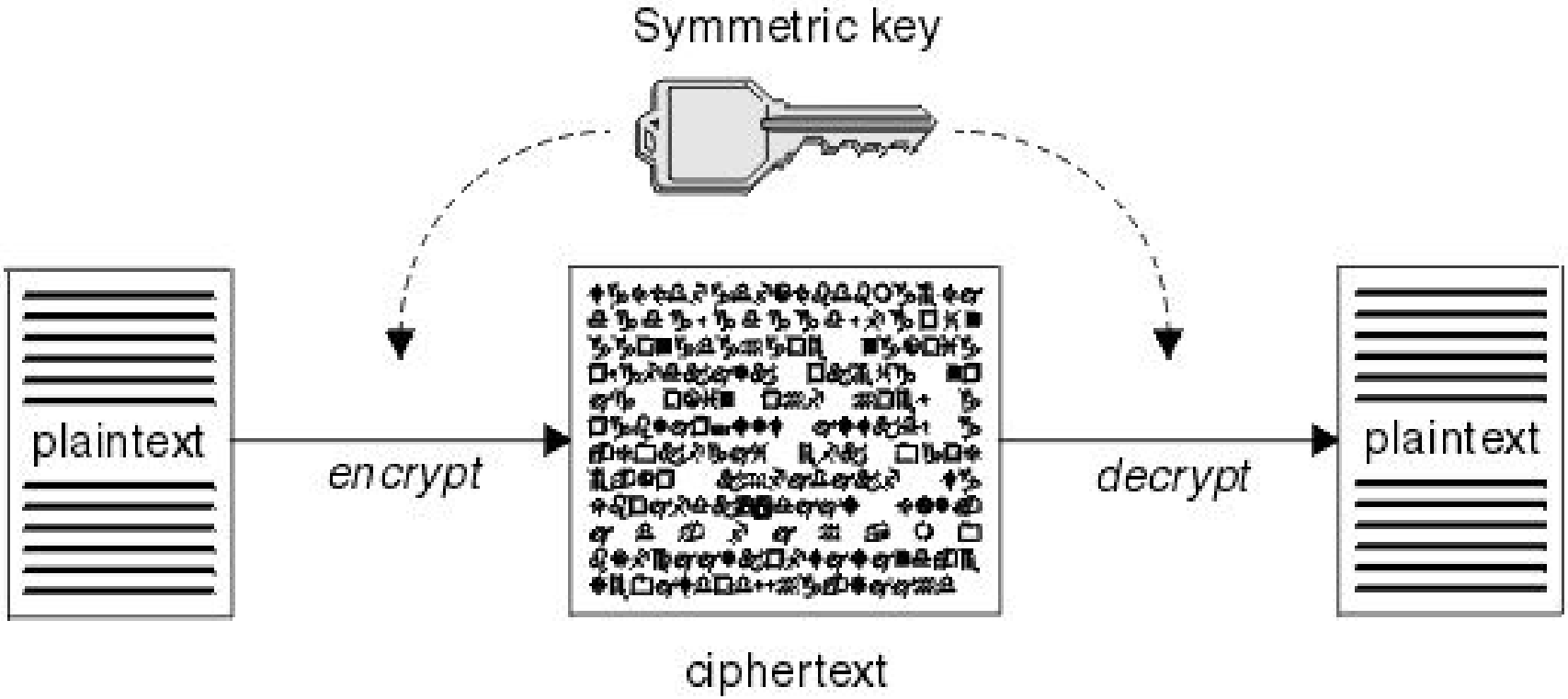
Nicht ins Flugzeug mitnehmen!

Sonder-Maschinenschlüssel BGS

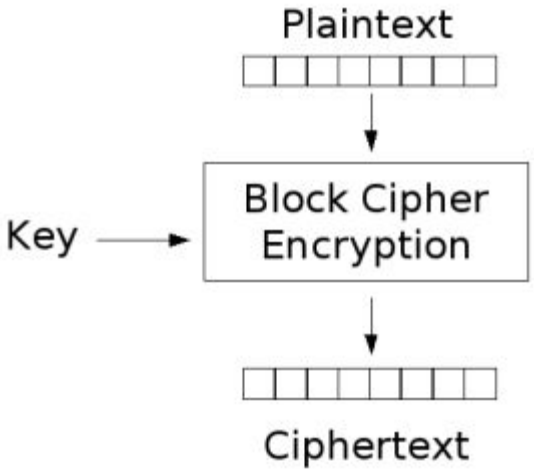
08 ❊

Datum	Walzenlage	Ringstellung	Steckerverbindungen	Kenngruppen
31.	I II V	10 14 02	BF SD AY HG OU QC WI RL XP ZK	yqv vuc xxo gvf
30.	V IV I	04 25 01	DI ZL RX UH QK PC VY GA SO EM	mqy vts gvt csx
29.	III V II	13 11 06	ZM BQ TP YX FK AR WH SO NJ DG	aky vdv oyo tzt
28.	I III II	09 16 12	NE MT RL OY HV IU GK FW PZ XC	nfh vcc tur wnb
27.	III II I	06 03 15	BF GR SZ OM WQ TY HE JU XN KD	bec jmv vtp xdb
26.	I III V	19 26 08	GS VD CQ LE HI BO JP UZ FT RN	wvu yem buz rjk
25.	II I IV	05 01 16	KA ZH QP GR MF LJ OT EN BD YW	ktv muq cqm cpm
24.	III II IV	22 02 06	PI KM JB YU QS OV ZA GW CH XF	zcd iwo urp glg
23.	IV III II	08 11 07	SX TD QP HU FB YN CO IK WE GZ	epm mgz vqg vsm
22.	I V II	13 02 26	GP XH IW BO NU MD SA ZK QR LT	aam mvy jqq wqm
21.	IV I V	17 24 03	XC AQ OT UZ HD RG KM BL NS JW	ltl blu frk xrh
20.	IV I III	15 22 12	PO TV QC ZS EX WR BJ DK FU LA	non lic oxr usr
19.	V I III	13 24 21	HA GM DI VK JP YU EF TB ZL XQ	ecd ciq uvr ppt
18.	IV V I	23 09 20	XF PZ SQ GR AJ UO CN BV TM KI	fjh zts uqu cft
17.	III II V	21 24 15	UT ZC YN BE PK JX RS GF IA QH	oub eci pyf rqi
16.	IV III V	07 01 13	IN YJ SD UV GF BH TK QE AR OP	kex paw flw onw
15.	I IV II	15 04 25	TM IJ VK OY NX PR WL GA BU SF	sdr pbu byv khb
14.	III II IV	10 23 21	WT RE PC FY JA VD OI HK NX ZS	mhz lff lnq giy
13.	V I II	14 04 12	AN IV LH YP WM TR XU FO ZB ED	rqh ucm ldi ods
12.	II V I	07 19 02	HR NC IU DM TW GV FB ZL EQ OX	asy xza uvc fmr
11.	I V IV	13 15 11	NX EO RV GP SU DK IT FY BL AZ	gyd iuq ocb vef
10.	V II I	09 20 19	FN TA YJ SO EG PC VD KI XH WZ	pyz ace pru uyc
9.	I IV V	14 10 25	VK DW LH RF JS CX PT YB ZG MU	nyh fbd ohs jrp
8.	IV V I	22 04 16	PV XS ZU EQ BW CH AO RL JN TD	tck rts nro mkl
7.	V I IV	18 11 25	TS IK AV QP HW FM DX NG CY UE	mhw lwb mdm ybe
6.	IV I III	02 17 20	KZ FI WY MP DS HR CU XE QV NT	uwu vdk lrh mgd
5.	I V IV	26 09 14	VW LT PB FO ZK GS RI QJ HM XE	suw tsy nfp yjc
4.	IV III V	07 01 12	QS YA XW KR MP HT DU OV CL FZ	uby usf mhh mwb
3.	I II V	05 16 03	FW DL NX BV KM RZ HY IQ EC JU	tns von grw axl
2.	III I II	12 22 17	DW UO PY GR FS EQ KT CL AI ZB	smz lbl bkc sym
1.	I III II	04 18 06	ZN OM CR UI KP WQ SE JV LX TF	ghr vqv cya ayl

Symmetric Key Encryption



Block Ciphers



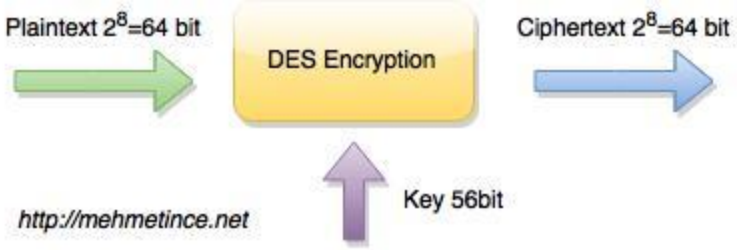
Block Ciphers

- Symmetric-key encryption ailesine aittirler.
- Fixed-lenght dediğimiz yaklaşım ile, plain-text ve key sabit uzunlukta gruplara bölünerek şifreleme işlemi gerçekleştirilmektedir.
- Anahtar ile cipher-text yani şifreli metin arasında herhangi bir ilişki kurulamamalıdır.
- Aynı şekilde cipher-text yani şifreli metine bakarak anahtar hakkında herhangi bir tahminde bulunulamıyor olmalıdır.
- Şifreli metin üzerinde yapılacak 1 bit'lik değişiklik bile plain-text'in en az %50'sinin değişmesine neden olmalıdır.

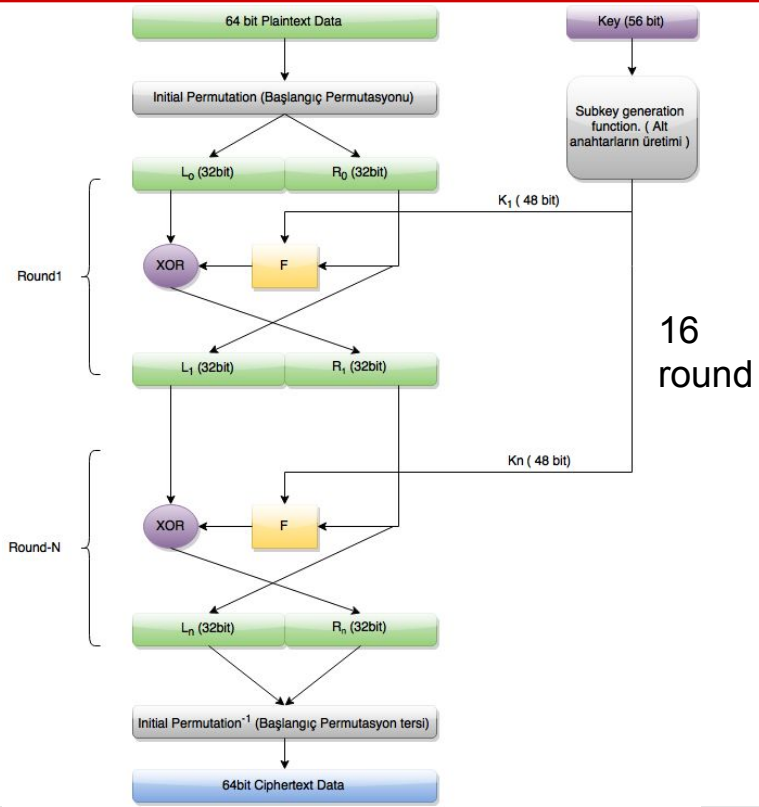
DES

IBM tarafından geliştirildi.

DES

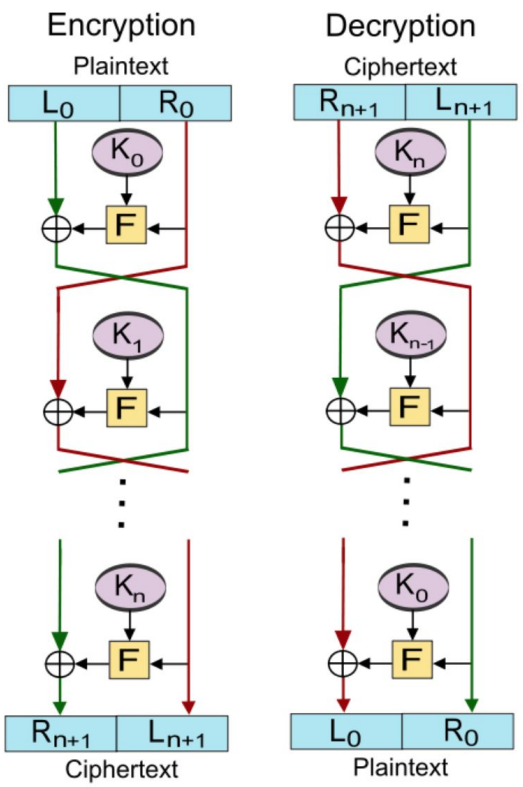

Plaintext 2^8=64 bit
DES Encryption
Ciphertext 2^8=64 bit
Key 56bit
http://mehmetince.net

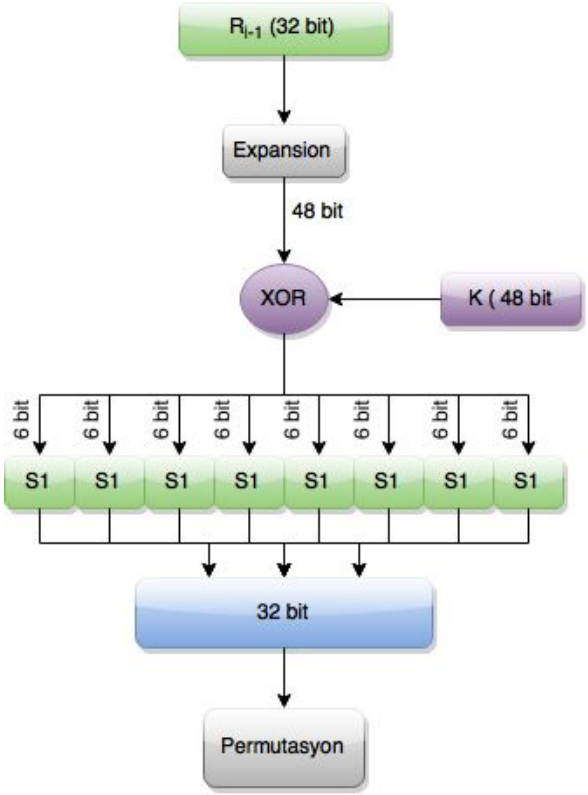
DES


64 bit Plaintext Data
Key (56 bit)
Initial Permutation (Başlangıç Permutasyonu)
Subkey generation function. (Alt anahtarların üretimi)
L_o (32bit)
R_0 (32bit)
K_1 (48 bit)
Round1
XOR
F
L_1 (32bit)
R_1 (32bit)
Kn (48 bit)
Round-N
XOR
F
L_n (32bit)
R_n (32bit)
Initial Permutation^{-1} (Başlangıç Permutasyon tersi)
64bit Ciphertext Data

16 round

DES


Encryption
Plaintext
L_0
R_0
K_0
F
K_1
F
K_n
F
R_{n+1}
L_{n+1}
Ciphertext
Decryption
Ciphertext
R_{n+1}
L_{n+1}
K_n
F
K_{n-1}
F
K_0
F
L_0
R_0
Plaintext


R_{i-1} (32 bit)
Expansion
48 bit
XOR
K (48 bit
6 bit
S1
32 bit
Permutasyon

DES

En başta 56 bitlik anahtardan 48 bit'lik alt-anahtarlar oluşturduk. Neden doğrudan 32 bitlik alt-anahtarlar yapıp direk 32 bitlik bloklar ile rahatça XOR işlemi yapmıyoruz ?

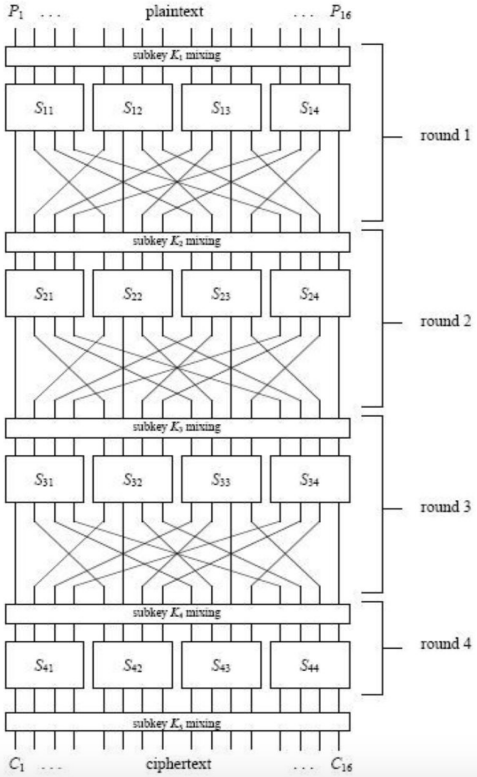
Triple DES

$$ciphertext = E_{K_3}\left(D_{K_2}\left(E_{K_1}(plaintext)\right)\right)$$

$$plaintext = D_{K_1}\left(E_{K_2}\left(D_{K_3}(ciphertext)\right)\right)$$

- Tüm anahtarlar bağımsız olabilir.
- K1 ve K2 birbirinden bağımsız K1=K3

AES - Advanced Key Standard



- Byte’lara böl
- Satırları kaydır
- Sütunların yerlerini değiştir
- Her adım için round anahtarı ekle

DES vs AES

	DES	AES
Yıl	1977	2000
Anahtar Uzunluk	56bits	128,196 or 256bits
Cipher Type	Simetrik	Simetrik
Block Size	64bits	128bits

RC4

Stream Cipher

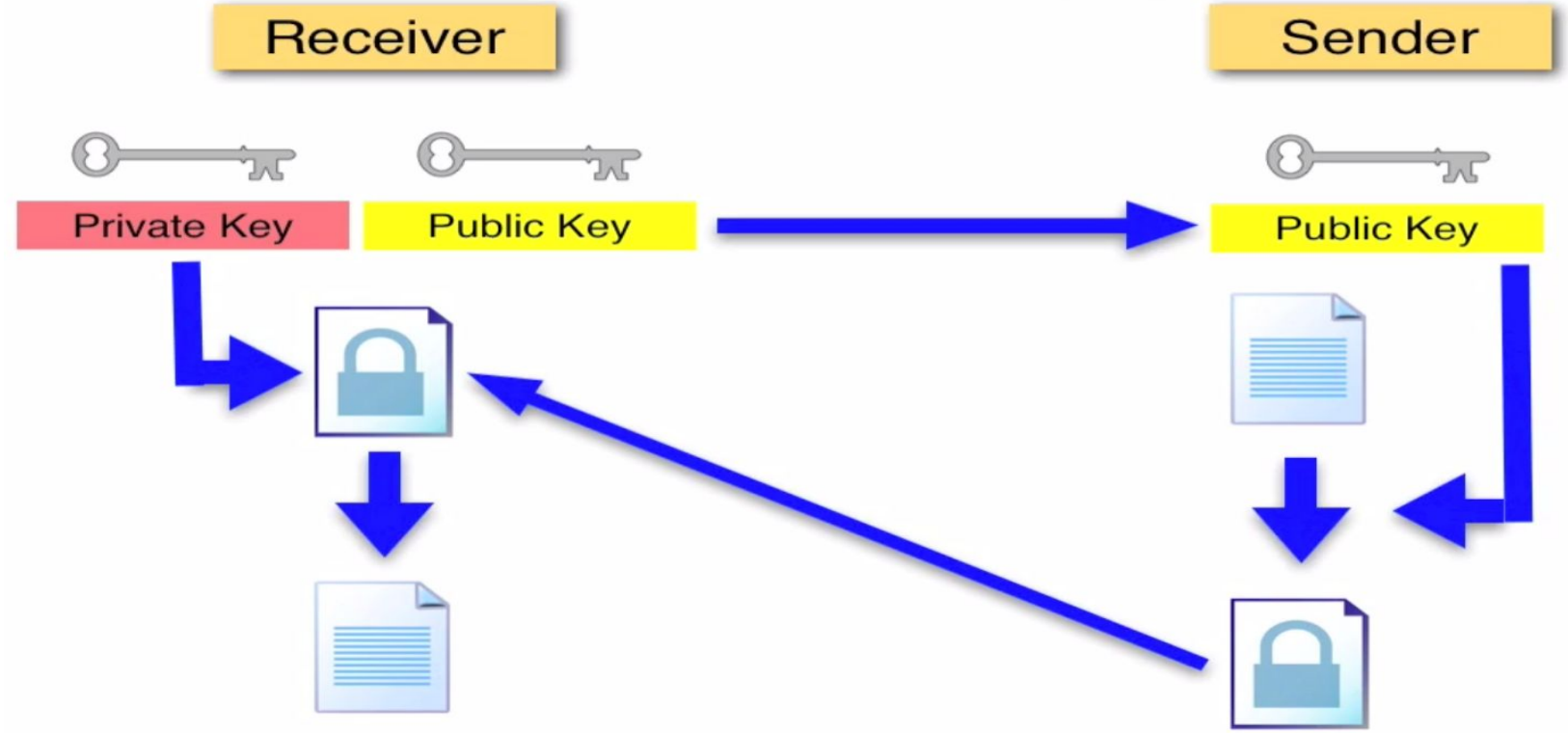
Anahtar

256 Round

40 - 2048 bit

- SSL, WEP, WPA...

Açık Anahtarlı Şifreleme

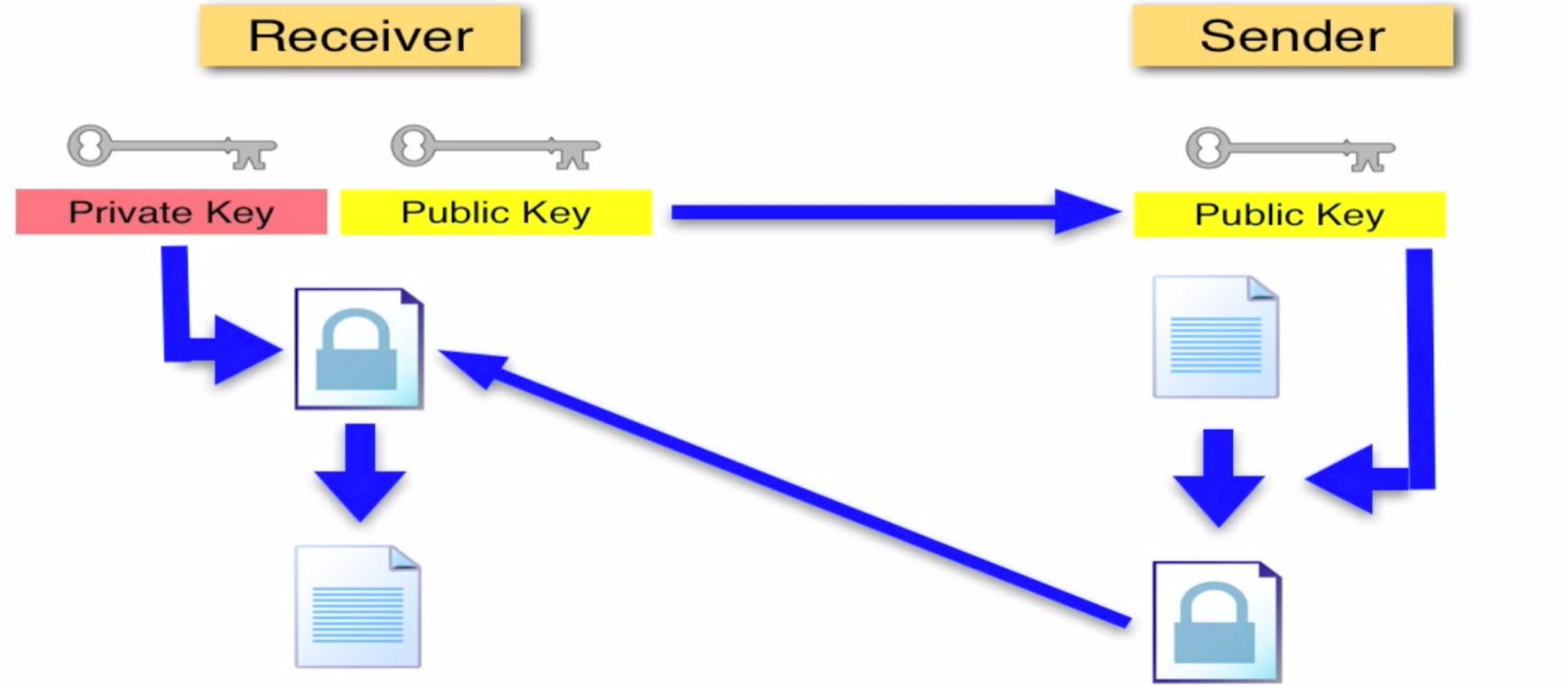


Diffie Hellman Key Agreement Prot.

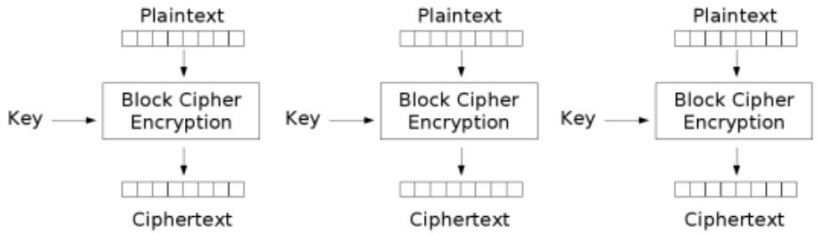
($f(X, Z)$: commutative one way function)

Alice		*Bob*
$Y_A = f(X_A, Z)$		
	$\xrightarrow{Y_A}$	
		$Y_B = f(X_B, Z)$
	$\xleftarrow{Y_B}$	
$K_{AB} = f(X_A, Y_B) = f(X_A, f(X_B, Z))$		$K_{BA} = f(X_B, f(X_A, Z))$

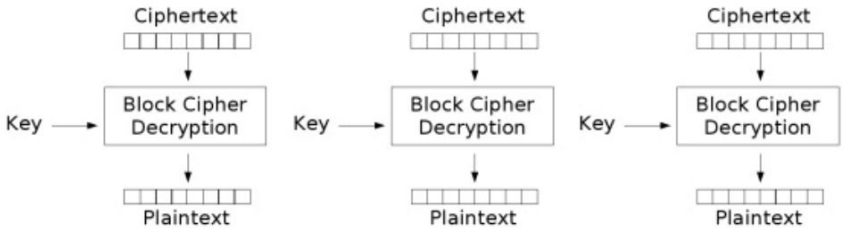
RSA



Mode'lar



Electronic Codebook (ECB) mode encryption

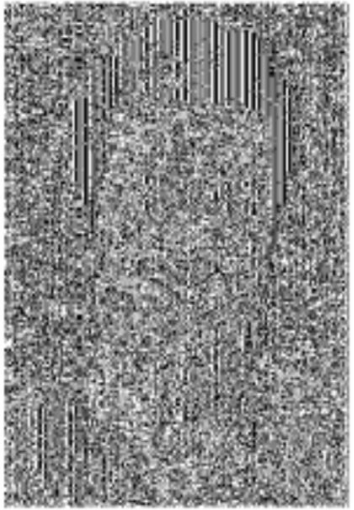


Electronic Codebook (ECB) mode decryption

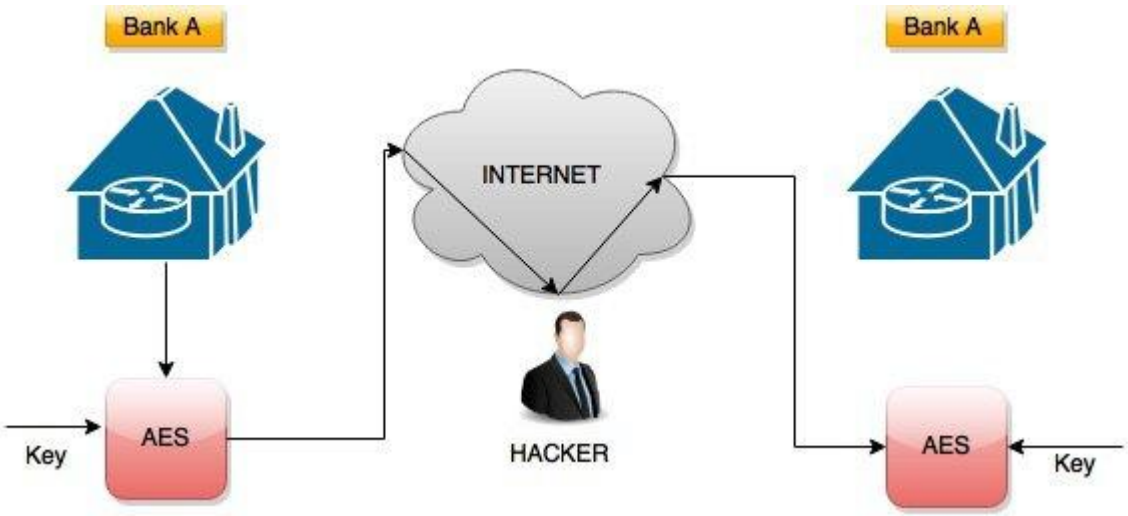
ECB

An example plaintext

Encrypted with AES in ECB mode

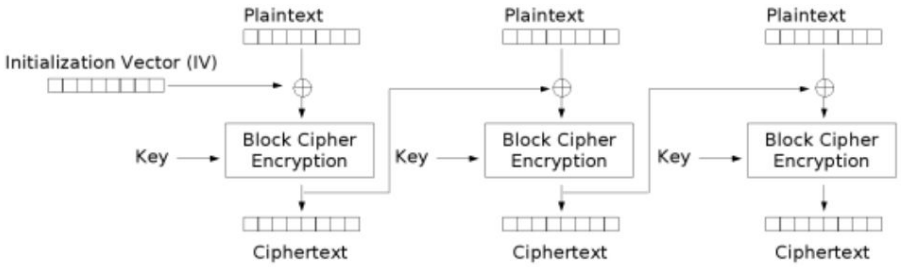


ECB

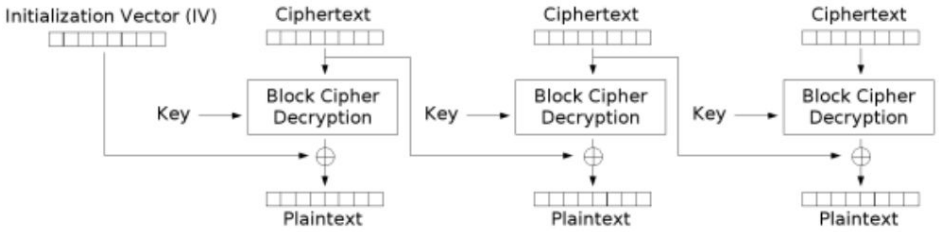

Bank A
Bank A
INTERNET
HACKER
Key
AES
AES
Key


BANK A
ACCOUNT #A
BANK B
ACCOUNT #B
AMOUNT

CBC - Cipher Block Chaining



Cipher Block Chaining (CBC) mode encryption

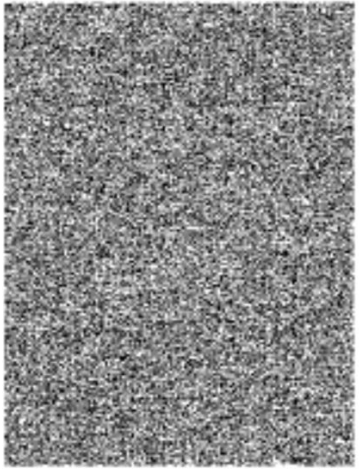


Cipher Block Chaining (CBC) mode decryption

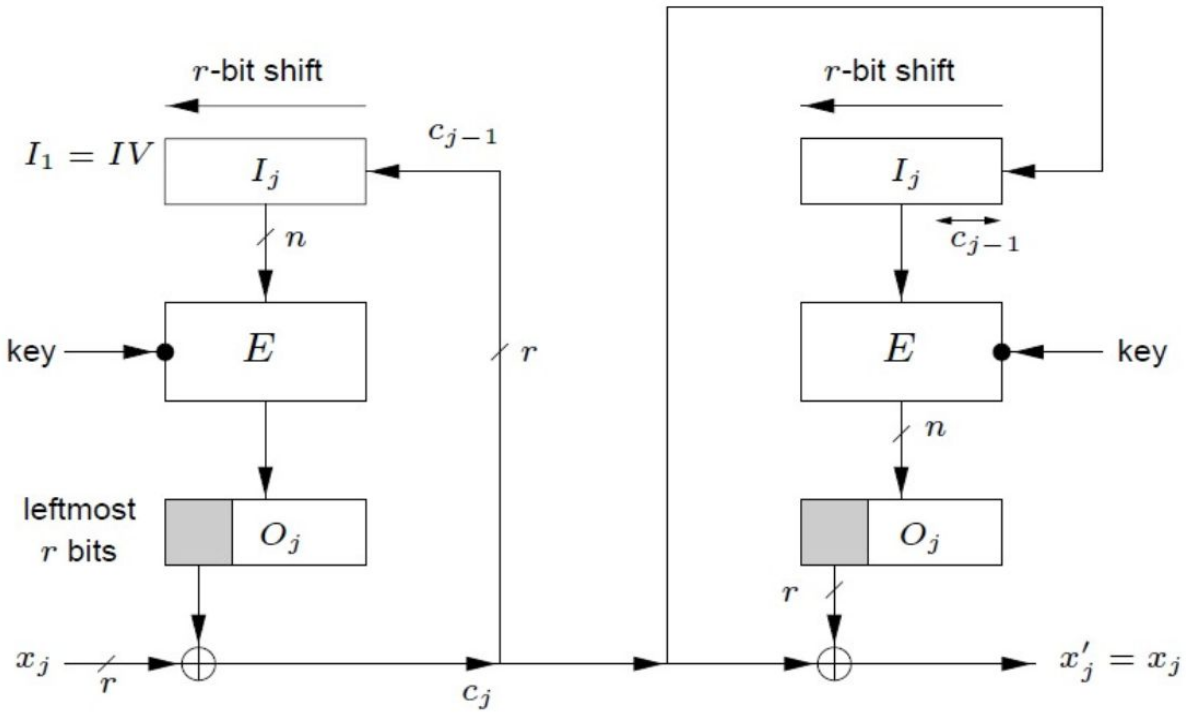
CBC with AES

An example plaintext

Encrypted with AES in CBC mode

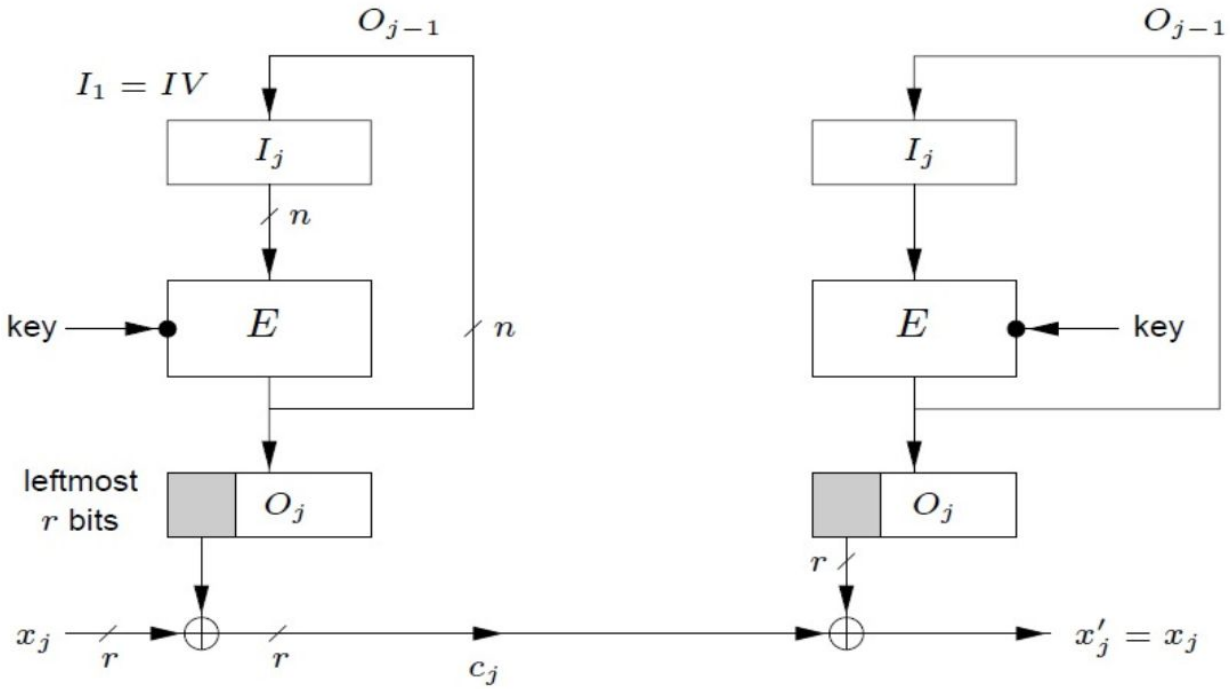


CFB - Cipher Feedback Block



(i) encipherment (ii) decipherment

OFB - Output Feedback Mode



Hash

İdeal bir hash fonksiyonu;

- Verilecek herhangi bir mesaj için kolayca oluşturulabilmeli
- Hash’ten mesaja geri dönebilmek mümkün olmamalı
- Mesajdaki en küçük değişiklik hash’i de değiştirmeli
- Aynı hash’e sahip birden çok mesaj bulunmamalı

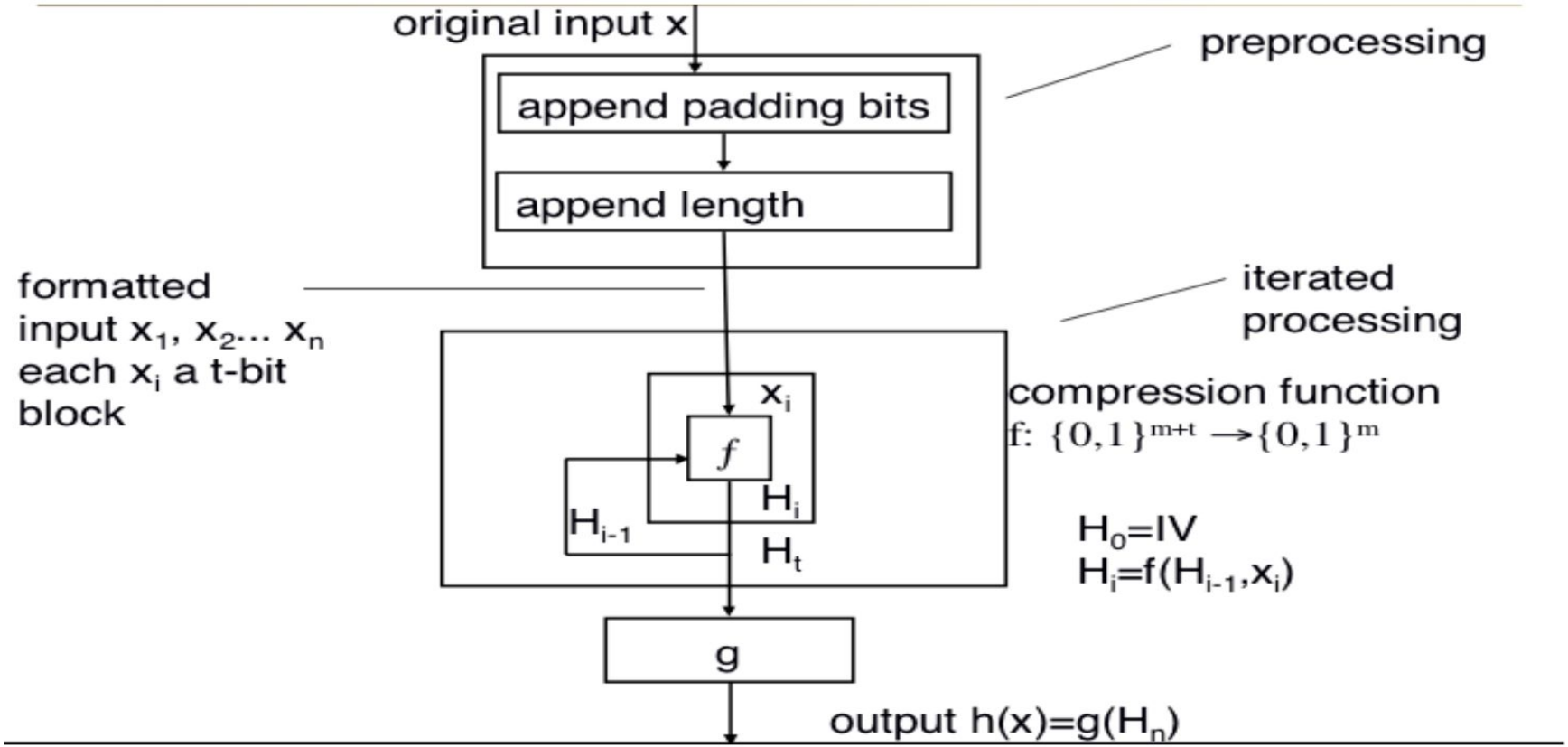
Hash Fonksiyonları İçin Güvenlik

1. **Preimage Resistance:** hash to input
2. **Second Preimage Resistance:** given x1 find x2

x1 != x2 h(x1)=h(x2)

3. **Collision Resistance:** any inputs x1, x2 h (x1)=h(x2)

Hash


original input x
preprocessing
append padding bits
append length
formatted
input $x_1, x_2 \ldots x_n$
each x_i a t-bit
block
iterated
processing
x_i
f
H_i
H_{i-1}
H_t
compression function
$f: \{0,1\}^{m+t} \rightarrow \{0,1\}^m$
$H_0=IV$
$H_i=f(H_{i-1},x_i)$
g
output $h(x)=g(H_n)$

Hash Algoritmaları

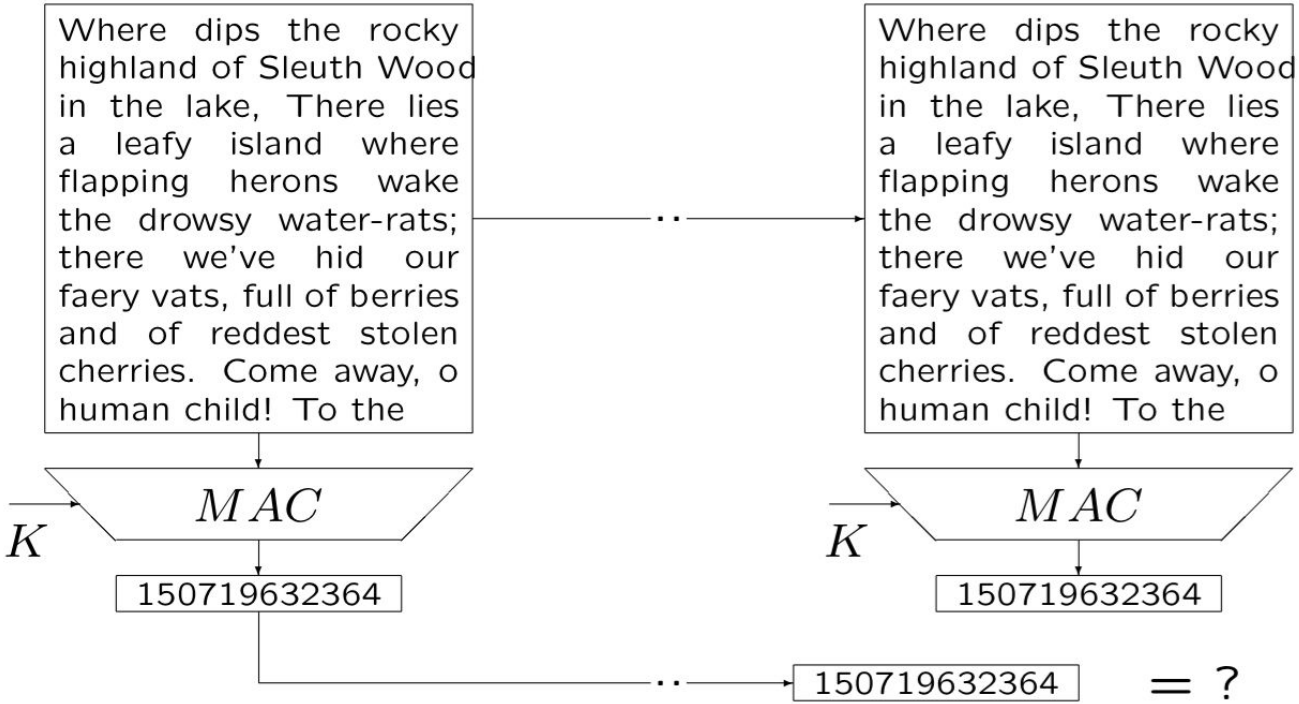
- SHA1 : 160 bits
- MD5 : 128 bits
- SHA3 : 224 256 384 512 bits
- MAC*
- HMAC

MD5 Collision

```
d131dd02c5e6eec4693d9a0698aff95c    2fcab58712467eab4004583eb8fb7f89
55ad340609f4b30283e488832571415a    085125e8f7cdc99fd91dbdf280373c5b
d8823e3156348f5bae6dacd436c919c6    dd53e2b487da03fd02396306d248cda0
e99f33420f577ee8ce54b67080a80d1e    c69821bcb6a8839396f9652b6ff72a70
```

```
d131dd02c5e6eec4693d9a0698aff95c    2fcab50712467eab4004583eb8fb7f89
55ad340609f4b30283e4888325f1415a    085125e8f7cdc99fd91dbd7280373c5b
d8823e3156348f5bae6dacd436c919c6    dd53e23487da03fd02396306d248cda0
e99f33420f577ee8ce54b67080280d1e    c69821bcb6a8839396f965ab6ff72a70
```

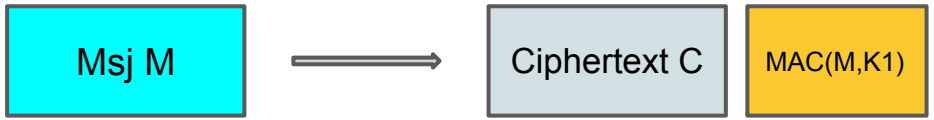
MAC


Where dips the rocky highland of Sleuth Wood in the lake, There lies a leafy island where flapping herons wake the drowsy water-rats; there we've hid our faery vats, full of berries and of reddest stolen cherries. Come away, o human child! To the
Where dips the rocky highland of Sleuth Wood in the lake, There lies a leafy island where flapping herons wake the drowsy water-rats; there we've hid our faery vats, full of berries and of reddest stolen cherries. Come away, o human child! To the
MAC
K
150719632364
MAC
K
150719632364
150719632364
= ?

MAC ve Encryption

- SSL - MAC sonra Encrypt

- SSH - Encrypt ve MAC



Ataklar

- Algebraic Attack
- Dictionary Attack
  - https://github.com/discourse/discourse/blob/master/lib/common_passwords/10k-common-passwords.txt
  - http://cyberwarzone.com/massive-collection-password-wordlists-recover-lost-password/
- Rainbow Table Attack