Information Security

Privacy ⟶ Only the intended recipient can see the contents of the communication or data. To be able to protect the network data we use SSL,https (uses SSL at the background) protocols.

Confidentiality⟶Protecting information from being accessed by unauthorized parties and disclosure.

Auditing⟶ Take a log of everything done in the system.

Availability⟶ Make the service available all the time.

Authorization⟶ Limit the resources that user can access. Passwords,smart cards,tokens,finger print

Notarization ⟶ assures the parties of a transaction that a document is authentic, and can be trusted.

Repudiation⟶Attackers often want to hide their malicious activity, to avoid being detected and blocked. They might therefore try to repudiate actions they have performed, for instance by erasing them from the logs, or by spoofing the credentials of another user.

Tampering⟶security threat faced by Web Applications. Data tampering is that act of deliberately modifying, manipulating or editing data through unauthorized channels. Basically only authorized users should be able to modify a system or the data it uses.

Non-Reputation ⟶ Protection against denial by one of the entities in a communication.

> **a)Origin non-repudiation:** Proof that message was sent by the entity
>
> **b)Destination non-repudiation:** Proof that message was received by the entity.

Integrity⟶Ensuring the data is read,accurate and guarded against unauthorized user modification(**Data integrity**). System performs as intended without any unauthorized access and operations(**System integrity**)

Secrecy→Controlling access to information from an entity that does have right to access.

Privacy→Controlling information from entity that does not generally have right of access

Dependability →Measure of system condition. Can we trust system as a whole.

Accountability→Traceability of actions performed on a system to a specific system entity.

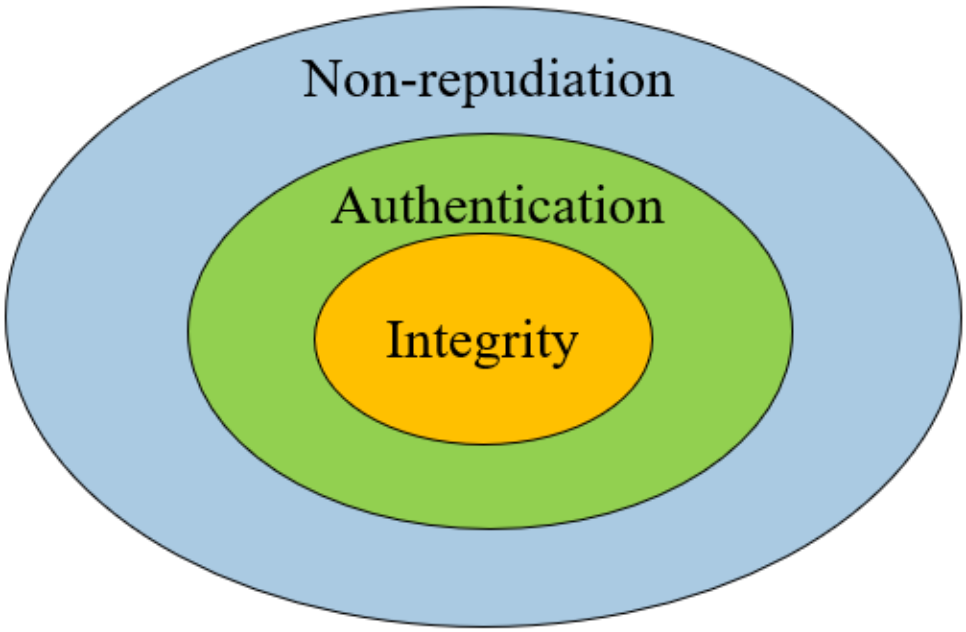
We can ensure that by;

1)Users have to be identified and authenticated to have a basis for access control decisions and to find out responsible entity in case of violation.

2)Security system keeps on audit(denetim) log of security relevant events to detect intrusions.

Relationships

among integrity, data-origin authentication and non-repudiation



!!!!Once you authenticated yourself,you cannot repudiate your identity.

!!!!!Authentication leads to non-repudiation.

Authenticity is about one party (say, Alice) interacting with another (Bob) to convince *Bob* that some data really comes from Alice.

Non-repudiation is about Alice showing to Bob a proof that some data really comes from Alice, such that not only Bob is convinced, but Bob also gets the assurance that he could show the same proof to Charlie, and Charlie would be convinced, too, even if Charlie does not trust Bob.

Secrecy(gizlilik) is a service ,**encryption** is a mechanism.

Steganography-Cryptography

- Steganography
  - hides the existence of a message
- Cryptography
  - hide the meaning of a message

Steganography de dummy content var bunun içinde gerçek bir mesaj var→ Prison break deki I am okay LJ gibi.

Cryptography de ise mesajı değil anlamını gizliyosun.

Steganography Sample

- Least significant bit values of pixels can be used to hide a secret message
  - Below images seem to be same but right picture store 5 Shakespeare games.

Hamlet, Macbeth, Julius Caesar
Merchant of Venice, King Lear

800×600 oldugunu düşünelim resmin 480000 civarında pixel var. Her bir pixel için red green blue kanallarını tutuyoruz. ve bu kanalların her biri için 1 byte tutuyoruz. Her byte da 8 bit. En küçük biti değiştirirsek ton çok değişmiyor ama insan gözü algılayamıyor.

Red green blue kanalları için 1 bit saklarsanız 1 pixelde 3 bit saklıyosun. Toplamda 1.5milyon biti bu görselde saklayabiliyosun

Cryptography-Cryptanalysis-Cryptology

- **Cryptography**: the study of mathematical techniques related to aspects of providing information security services.
- **Cryptanalysis**: the study of mathematical techniques for attempting to defeat information security services.
- **Cryptology**: the study of cryptography and cryptanalysis.

There are different methods of breaking a cipher, depending on:

- the type of information available to the attacker
- the interaction with the cipher machine
- the computational power available to the attacker

CipherText only attack : Only knows cyphertext. Find the plaintext and key. Eğer bir encryption scheme ciphertext attack için savunmasız ise buna completely

insecure deriz.

KnownPlainText attack : Plaintext var ciphertext var keyi bulmaya çalışıyosun.

ChosenPlainText attack: Send many plain text and obtain cipher texts. Sonra da key'i bulmaya çalış.

ChosenCipherText attack: Ciphertext var elinde onları decrypt edip plain text elde edip keyi bulmaya çalış.

Shift Cipher

Caesar's Cipher

-Both sender and receiver agree on a secret shift number.

-Replace each letter by one with 3 letter(circularly) down, or number fixed a→d,b →e...

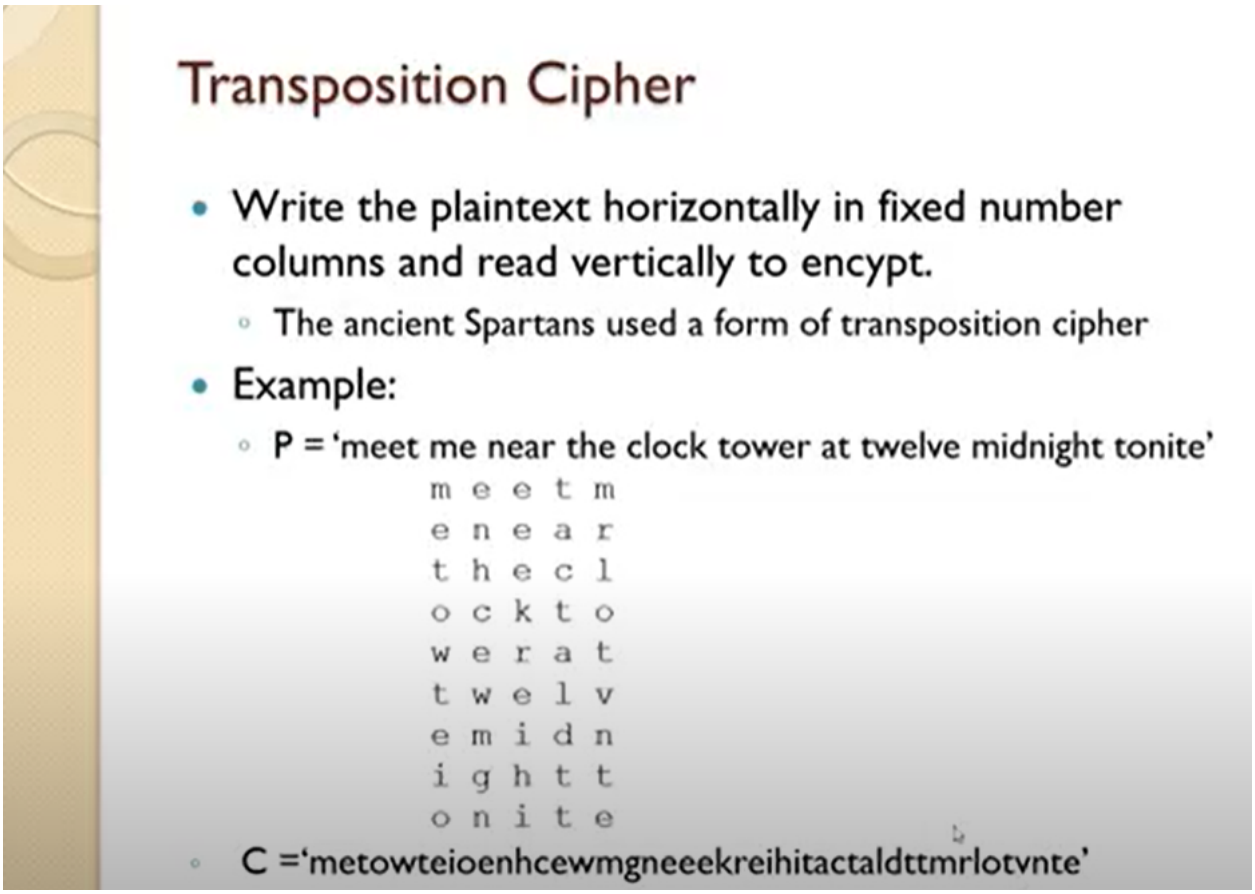
-No key

-Substitution technique

-Since there are 26 possible shift,brute force easily break it.

-selected key must be between [1-25]

Transposition



Monoalphabetic ciphers

-A monoalphabetic substitution cipher, also known as a simple substitution cipher, relies on a fixed replacement structure. That is, the substitution is fixed for each letter of the alphabet. Thus, if "a" is encrypted to "R", then every time we see the letter "a" in the plaintext, we replace it with the letter "R" in the ciphertext.

-Uses a fixed Substitution over the entire message

– shuffle the letters arbitrarily based on a 26 letters long key

```
Plain:  abcdefghijklmnopqrstuvwxyz
Cipher: DKVQFIBJWPESCXHTMYAUOLRGZN

Plaintext:  ifwewishtoreplaceletters
Ciphertext: WIRFRWAJUHYFTSDVFSFUUFYA
```

–26! = 4∗10 26 different keys

–but still insecure due to redundancies in the natural languages

some letters or letter pairs/triples occur more than others

-Frequency analysis made substitution cipher insecure.

How to increase the security of substitution cipher

Using nulls

- e.g., using numbers from 1 to 99 as the ciphertext alphabet, some numbers representing nothing are inserted randomly

Deliberately misspell words

- e.g., “Thys haz thi ifekkt off diztaughting thi ballans off frikwenseas”

Homophonic substitution cipher

- each letter is replaced by a variety of substitutes

Polyalphabetic substitution ciphers

Vigenere Cipher

Vigenère cipher is vulnerable: once the key length is found, a cryptanalyst can apply frequency analysis.

For Vigenere, as the length of the keyword increases, the letter frequency shows less English-like characteristics and becomes more random.

The Vigenère Cipher

- **Definition:**
  - Given m, a positive integer, $P = C = (Z_{26})^n$, and $K = (k_1, k_2, \ldots, k_m)$ a key, we define:
- **Encryption:**
  - $E_k(p_1, p_2 \ldots p_m) = (p_1+k_1, p_2+k_2 \ldots p_m+k_m) \pmod{26}$
- **Decryption:**
  - $D_k(c_1, c_2 \ldots c_m) = (c_1-k_1, c_2-k_2 \ldots c_m-k_m) \pmod{26}$

Example:

Plaintext:	C	R	Y	P	T	O	G	R	A	P	H	Y
Key:	L	U	C	K	L	U	C	K	L	U	C	K
Ciphertext:	N	L	A	Z	E	I	I	B	L	J	J	I

Polyalphabetic substitution ciphers

- different monoalphabetic substitutions as proceeding through the plaintext
- key determines which monoalphabetic substitution rule to be applied to each letter

Famous example is Vigenère cipher

```
key:        deceptivedeceptivedeceptive
plaintext:  wearediscoveredsaveyourself
ciphertext: ZICVTWQNGRZGVTWAVZHCQYGLMGJ
```

makes cryptanalysis harder

- multiple ciphertext letters for each plaintext letter
- frequency distribution is kind of obscured, but cryptanalysis is still possible

Vigenere Table

Vigenere Table

Table 2.3 The Modern Vigenère Tableau

	Plaintext																									
	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

Kasisky Test

- Two identical segments of plaintext will be encrypted to the same ciphertext, if the they occur in the text at the distance Δ, (Δ≡0 (mod m), m is the key length).
- Algorithm:
  - Search for pairs of identical segments of length at least 3
  - Record distances between the two segments: Δ1, Δ2, …
  - m divides gcd(Δ1, Δ2, …)

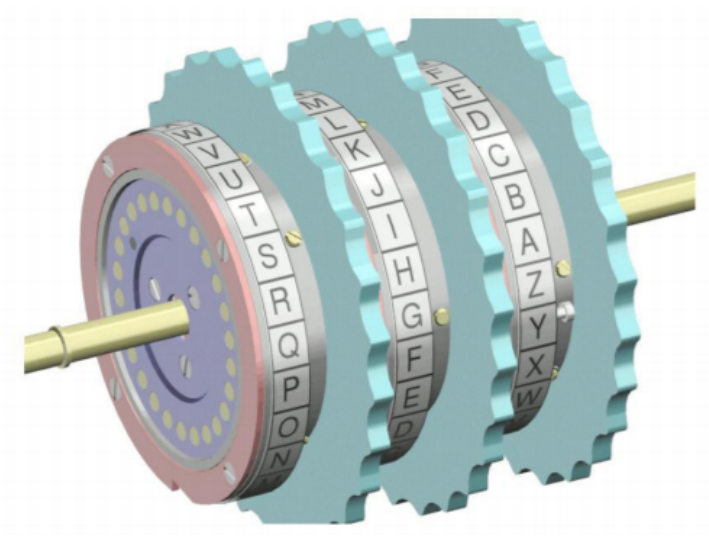
PT	T	H	E	S	U	N	A	N	D	T	H	E	M	A	N	I	N	T	H	E	M	O	O	N
Key	K	I	N	G	K	I	N	G	K	I	N	G	K	I	N	G	K	I	N	G	K	I	N	G
CT	D	P	R	Y	E	V	N	T	N	**B**	**U**	**K**	**W**	I	A	O	X	**B**	**U**	**K**	**W**	W	B	T

B ler arasında 8 var bu demek oluyoki keyin uzunluğu 8 in katı veya 8 i bölebilen bir sayı. 4 veya 8 . 2 olamaz çünkü 4 lü şekilde tekrar ediyor bloklar.

Rotor Machine

A machine consists of multiple cylinders
◦ each cylinder has 26 states, at each state it is a substitution cipher: the wiring between the contacts implements a fixed substitution of letters
◦ each cylinder rotates to change states according to different schedule changing the substitution

- A m-cylinder rotor machine has 26^m different substitution ciphers
  - $26^3 = 17576$
  - $26^4 = 456,976$
  - $26^5 = 11,881,376$

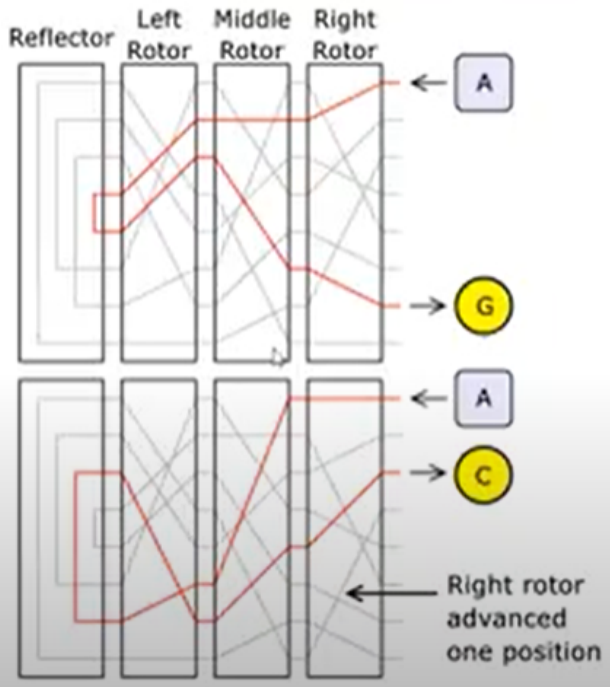


Enigma

- Use 3 scramblers (rotors): 17576 substitutions
- 3 scramblers can be used in any order: 6 combinations
- Plug board: allowed 6 pairs of letters to be swapped before the scramblers process started and after it ended.
- Total number of keys ≈ 10^{16}
- Later versions use 5 rotors and 10 pairs of letters

Key Mapping

- A reflector enables to map a character twice with each rotor
- First rotor rotates after each key press
- Second rotor rotates after first had a complete revolution,
- and so on



- Daily key: The settings for the rotors and plug boards changed daily according to a codebook received by all operators
  - A day key has the form
    - Plugboard setting: A/L–P/R–T/D–B/W–K/F–O/Y
    - Scrambler arrangement: 2-3-1
    - Scrambler starting position: Q-C-W
- Message key: Each message was encrypted with a unique key defined by the position of the 3 rotors

How to Break the Enigma Machine?

- Recover 3 secrets
  - Internal connections for the 3 rotors
  - Daily keys
  - Message keys

Kerckhoffs's Principle

The security of a protocol should rely only on the secrecy of the keys, protocol designs should be made public.

Anahtar güvenliğini sağla algoritmalar public olmalı.

OTP(One-time-pad) ⟶ Encryption technique that cannot be cracked but requires the use of one-time pre-shared key the same size or longer than the message being sent

-Secret key must be at least as long as the message

-Hard to use while sending large electronic information

-All bytes of the message are added XOR to bytes of the secret key. and each addition produces one output byte.

-Each part of the secret key can be used only once for encrypting one part of the message that's why the key must be at least as long as the message.

-Using the same key bytes more than once,allows attacker to discover the two original messages summed my XOR

M1 XOR K = C1

M2 XOR K = C2

Feistel Network

Feistel Ağı

Feistel ağında, şifrelenecek olan şifresiz metin bloğu iki eşit uzunluktaki parçaya ayrılır. Alt anahtar kullanılarak raund fonksiyonu bu yarımlardan birine uygulandıktan sonra öteki yarı ile XOR'lanır. Ardından iki yarı yer değiştirir.

$\mathbf{F}$ raund fonksiyonu olsun, ve $0, 1, \ldots, n$ için sırasıyla $K_0, K_1, \ldots, K_n$ alt anahtarlar olsun.

Basit işleyiş şu şekildedir:

Şifresiz metin bloğu iki eşit uzunluktaki parçaya ayrılır, (L_0, R_0)

$i = 0, 1, \ldots, n$ numaralı her raund için

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

hesapla.

Sonrasında (R_{n+1}, L_{n+1}) şifreli metindir.

(R_{n+1}, L_{n+1}) şifreli metnini çözme işlemi, $i = n, n-1, \ldots, 0$ için sırasıyla

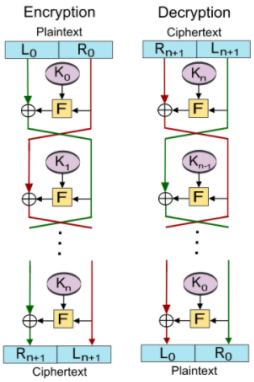
$$R_i = L_{i+1}$$
$$L_i = R_{i+1} \oplus \mathbf{F}(L_{i+1}, K_i)$$

hesaplanmasıyla elde edilir.

Ardından (L_0, R_0) şifresiz metindir.

Feistel ağının subtitüsyon-permutasyon ağına göre bir avantajı ise $\mathbf{F}$ raund fonksiyonun tersinin olma zorunluluğunun olmamasıdır.

anahtarları K_i'dır.



DES ve Blowfish gibi birçok blok şifrede Fiestel ağ yapısı kullanılmıştır.

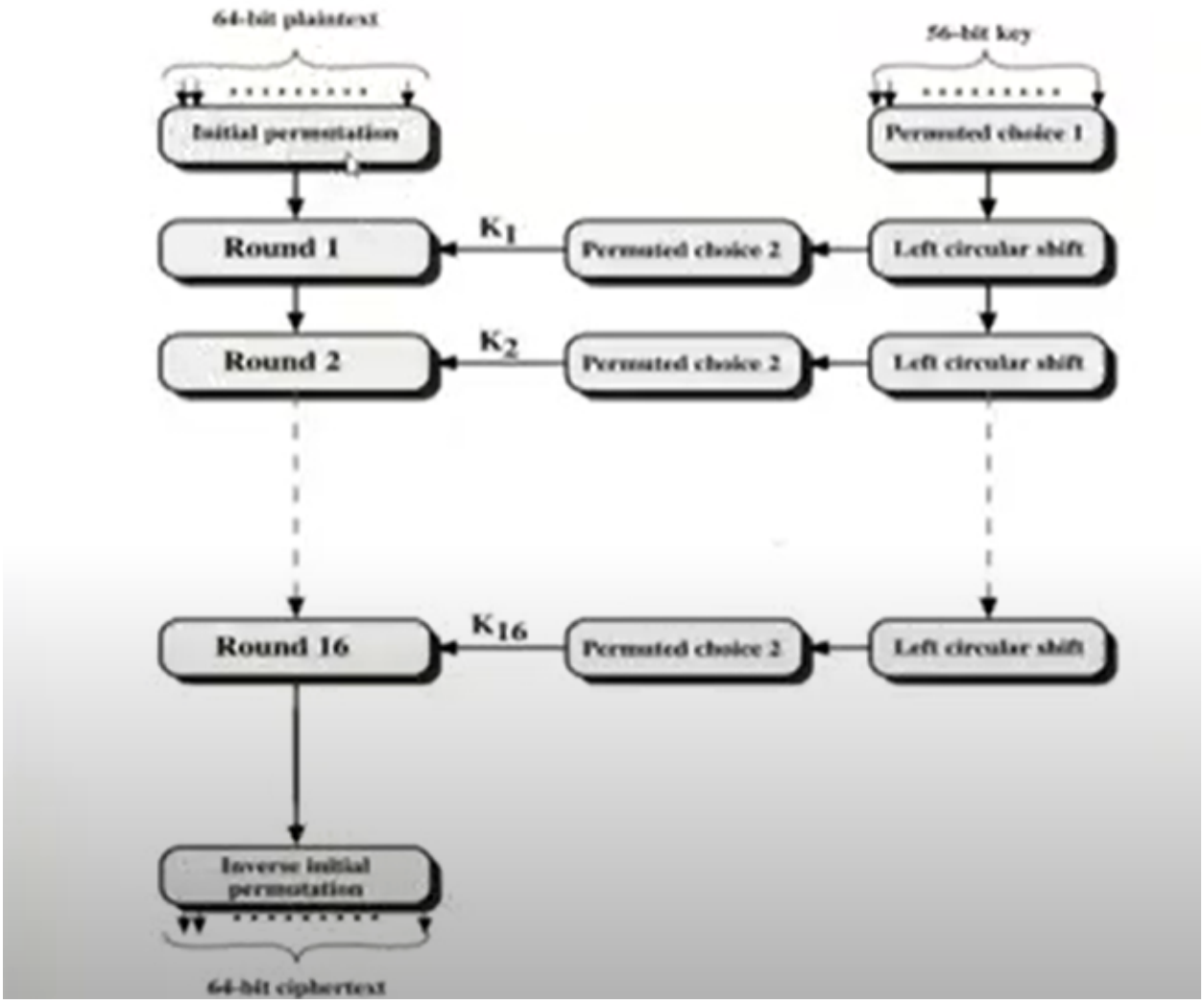
Hill Cipher

A Simple Block Cipher: Hill Cipher

- The key k is a matrix. The message is considered as vectors. Encryption and decryption operations are matrix multiplication operations
  - Encryption: $C = k.P \pmod{26}$
  - Decryption: $P = k^{-1}.C \pmod{26}$
- Example: The plaintext is `CAT` converted to numeric values, namely 2, 0, 19.
- If the key is $\begin{pmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{pmatrix}$
- Encryption: $\begin{pmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{pmatrix} \begin{pmatrix} 2 \\ 0 \\ 19 \end{pmatrix} \equiv \begin{pmatrix} 31 \\ 216 \\ 325 \end{pmatrix} \equiv \begin{pmatrix} 5 \\ 8 \\ 13 \end{pmatrix} \pmod{26}$
- C=`FIN`

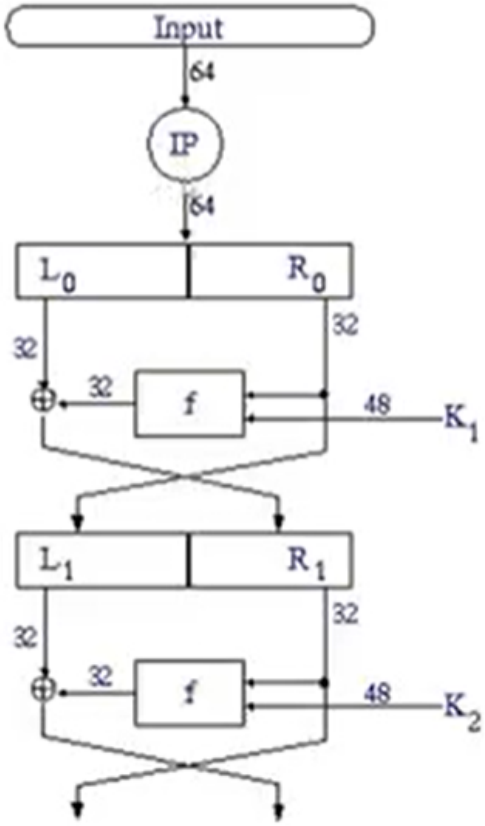
DES

DES Structure



- An initial permutation is applied on the plaintext
  $IP(x) = L_0 R_0$

- In each round:
  $L_i = R_{i-1}$
  $R_i = L_{i-1} \oplus f(R_{i-1}, K_i)$



After the last round

$y = IP^{-1}(R_{16}L_{16})$

f = round function in des. Bu fonksiyonda 32 bitlik valuğu 48 e expand ediyosun. Bunu da mesela 1.biti alıp 33 e yazıyosun 8.biti alıp 34 e yazıyosun yani 48 bit'e tamamlıyosun.Bu 48 bitlik valueyuda 8 e bölüyosun. 6 bitlik blocklar oluşuyo bunlarıda s box'a veriyosun. Bu box 6 biti 4 e indiriyo.

-most widely used block cipher in world

-encrypts 64 bit data using 56 bit key

Block size = 64 bits

- Key size = 56 bits
- Number of rounds = 16
- 16 intermediary keys, each 48 bits

- Weak keys: keys make the same sub-key to be generated in more than one round.
  - Result: reduce cipher complexity
  - Weak keys can be avoided at key generation. DES has 4 weak keys:

    0000000 0000000
    0000000 FFFFFFF
    FFFFFFF 0000000
    FFFFFFF FFFFFFF

- Semi-weak keys: A pair of DES semi-weak keys is a pair (K_1,K_2) with $E_{K_1}(E_{K_2}(x))=x$
- There are six pairs of DES semi-weak keys

Dictionary Attack to DES

- Even without having weak/semi-weak keys DES is vulnerable to dictionary attacks:
- Each plaintext may result in 2^{64} different ciphertexts, but there are only 2^{56} possible different key values.
- Given a PT/CT pair *(M,C)*
  - Encrypt the known plaintext M with all possible keys.
  - Keep a look up table of size 2^{56}.
  - Look up C in the table

Meet-in-the-middle-attack

Meet-in-the-middle Attack

- Goal: given the pair (P, C) find keys K_1 and K_2.
- Based on the observation:

$$C = E_{K2}[E_{K1}[P]]$$
$$D_{K2}[C] = E_{K1}[P]$$

1. Encrypt P with all 2^{56} possible keys K_1
   - Store all pairs (K_1, $E_{K1}[P]$), sorted by $E_{K1}[P]$.
2. Decrypt C using all 2^{56} possible keys K_2
   - For each decrypted result, check to see if there is a match $D_{K2}(C) = E_{K1}(P)$. If a match is found, (K_1 ,K_2) is a possible match
3. The attack has a higher chance of succeeding if another pair (P', C') is available to the cryptanalysis.

toplamda 2^57 tane operation 2^56+2^56 (encrypt and decrypt)

3DES

Two key version is widely used and standard
◦ Key space is 56 x 2 = 112 bits
Encrypt: C = EK1 [DK2 [EK1 [P]]]
Decrypt: P = DK1 [EK2 [DK1 [C]]]
Three key version is possible but not standard
◦ Key space is 56 x 3 = 168 bits
Encrypt: C = EK3 [DK2 [EK1 [P]]]
Decrypt: P = DK1 [EK2 [DK3 [C]]]

-Method for strong cipher

-Use multiple encyrption with DES with different keys

-Three stages of DES

a)2 different keys

b)3 different keys;complexity increases and becomes impractical

I have a triple DES key. What are its sub-keys?

Just split the 192-bit triple DES key into 3 separate 64-bit keys, working from left to right. For example, if your triple-DES key is the 192-bit value (in hex format):

```
0123456789ABCDEFFEDCBA987654321089ABCDEF01234567
```

then split it into the three sub-keys, K1, K2 and K3, each of 64 bits:

```
 0123456789ABCDEF FEDCBA9876543210 89ABCDEF01234567
|<------K1------>|<------K2------>|<------K3------>|
```

So the sub-keys are K1=`0x0123456789ABCDEF`, K2=`0xFEDCBA9876543210` and K3=`0x89ABCDEF01234567`.

Can I do single-key DES encryption with a Triple DES function?

If you encrypt something, then decrypt it and encrypt it again with the same key, you've just done the same as encrypting it once. Thus option 3 with three identical keys is simply the original 64-bit DEA algorithm with a keyspace of 56 bits, albeit done with three times as much effort. So, to carry out "single" DES using a Triple DES function, just set all three DEA keys to be the same. Note that this option is no longer permitted under NIST SP 800-67.

For example, if your single-DES key is `0x89ABCDEF01234567` then set your Triple-DES key to be

```
 89ABCDEF01234567 89ABCDEF01234567 89ABCDEF01234567
|<------K1------>|<------K2------>|<------K3------>|
```

What's two-key triple DES encryption?

Two-key triple DES is option 2 where we encrypt with K1, then decrypt with K2 and finally encrypt again with K1. The keyspace is thus 2 x 56 = 112 bits.

For example, with K1=`0x0123456789ABCDEF` and K2=`0xFEDCBA9876543210` you would set the triple DES key to be `0x0123456789ABCDEFFEDCBA98765432100123456789ABCDEF`.

```
 0123456789ABCDEF FEDCBA9876543210 0123456789ABCDEF
|<------K1------>|<------K2------>|<------K3------>|
```


What's two-key triple DES encryption?

Two-key triple DES is option 2 where we encrypt with K1, then decrypt with K2 and finally encrypt again with K1. The keyspace is thus 2 x 56 = 112 bits.

For example, with K1=`0x0123456789ABCDEF` and K2=`0xFEDCBA9876543210` you would set the triple DES key to be `0x0123456789ABCDEFFEDCBA98765432100123456789ABCDEF`.

```
 0123456789ABCDEF FEDCBA9876543210 0123456789ABCDEF
|<------K1------>|<------K2------>|<------K3------>|
```


How long is a triple DES key: 192 or 168 bits?

As mentioned above, a triple DES key is a bundle of three DES keys. A DES key is 64 bits long, but only 56 bits of these are used in the encryption process.

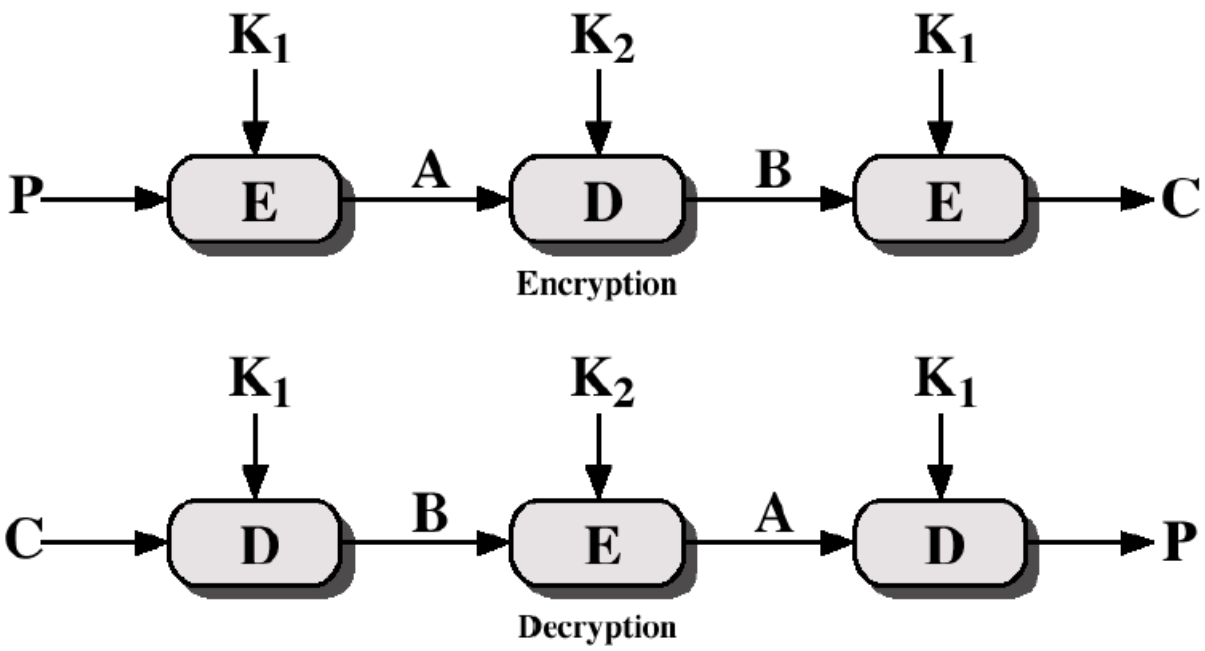
A triple DES key is therefore 3 x 64 = 192 bits long, but the *keyspace* is only 3 x 56 = 168 bits.

Note that if your "triple DES" key is not exactly 192-bits long - i.e. exactly 24 bytes long, or 48 hexadecimal digits - then you do not have a valid triple DES key.

The other 8 bits are meant to be used as error detecting or "parity" bits so, in principle, the validity of the key bit string can be checked (every byte should be of odd parity), but this is hardly ever done. Most people and most software packages, including **CryptoSys API** and **CryptoSys PKI**, do not bother to check the parity of the key and just ignore the state of the parity bits. Be careful, though, because this means that the keys represented, for example, by the following bit strings are treated as being equal, and will produce identical ciphertext output for the same plaintext input:

```
0123456789ABCDEF FEDCBA9876543210 89ABCDEF01234567
0022446688AACCEE FFDDBB9977553311 88AACCEE00224466
```

3DES with 2 keys

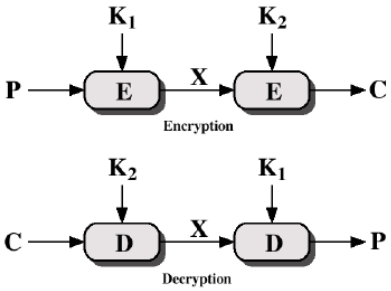


-Keys are 64 bits but only 56 bits of these are used in the encryption process.

3DES with 3 keys is not more secure than 3DES with two keys. using 3 keys are more slower.

Why not double DES?

Why not double DES?



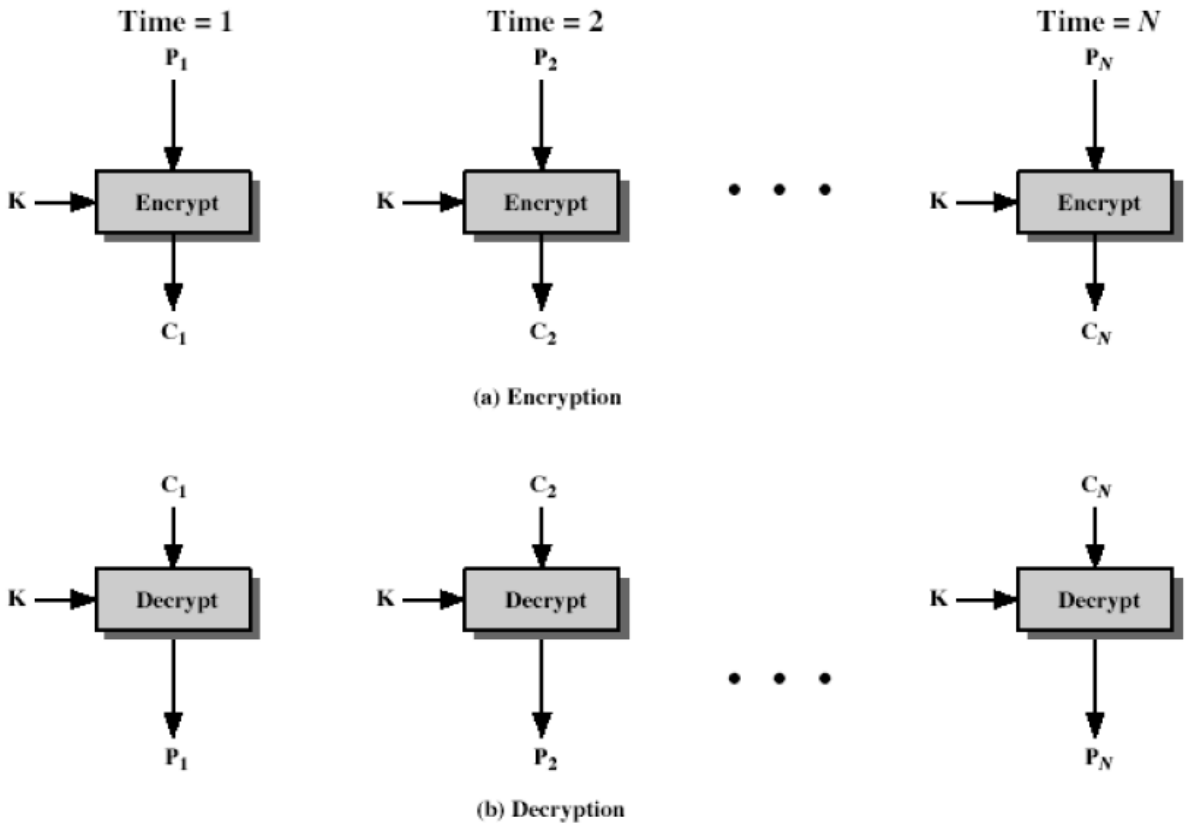
- Double DES
  - use DES two times with two different keys
  - Does not work due to meet-in-the-middle attack (which is a known-plaintext attack)
    - $X = E_{K1}[P] = D_{K2}[C]$
    - Try all possible K1's on P to create all possible X's and store them sorted
    - Try all possible K2's on C and match with above table
    - may create some false-alarms, so do the same attack for another plaintext-ciphertext pair
    - If the same K1-K2 pairs match for the second plaintext-ciphertext pair, then the correct keys are most probably found
    - complexity of this attack is close to the complexity of the single-DES brute-force attack, so double-DES is useless

Electronic Codebook Book (ECB) Mode of DES

Message is broken into independent blocks of block_size bits.

-each block is encrypted independent of the other blocks ;using the same key.

-Parallel encryption is possible.



the same data block gets encrypted the same way. This reveals patterns of data when a data block repeats

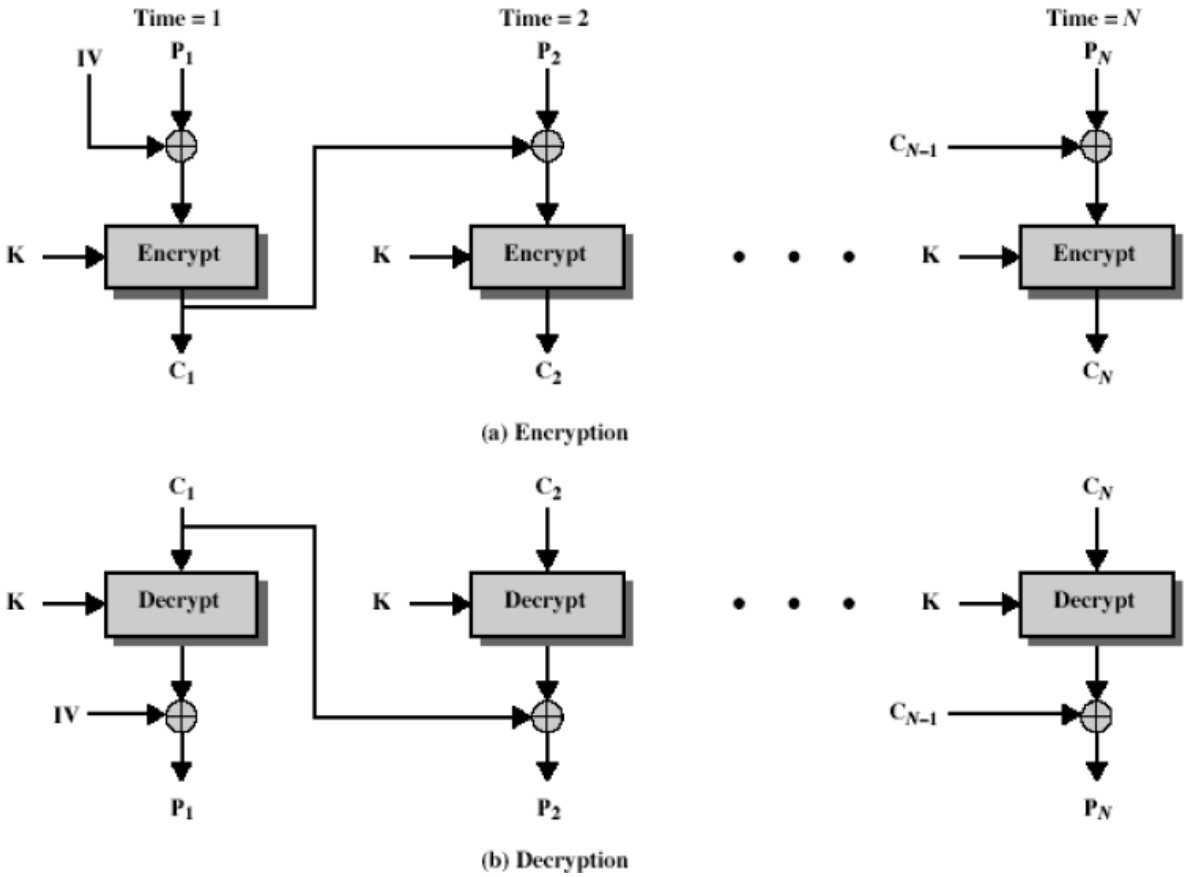
Malleable: reordering ciphertext results in reordered plaintext.

Cipher Block Chaining (CBC)

-each previous cipher blocks is XORed with current plaintext
-each ciphertext block depends on other message blocks
-need Initialization Vector (IV) known to sender & receiver

Randomized encryption: repeated text gets mapped to different encrypted data. can be proven to be “secure” assuming that the block cipher has desirable properties and that random IV’s are used

No parallel encryption



Initialization Vector (IV)

-Max security,it should be protected for unauthorized changes. Otherwise attackers change in IV also changes decrypted plaintext.

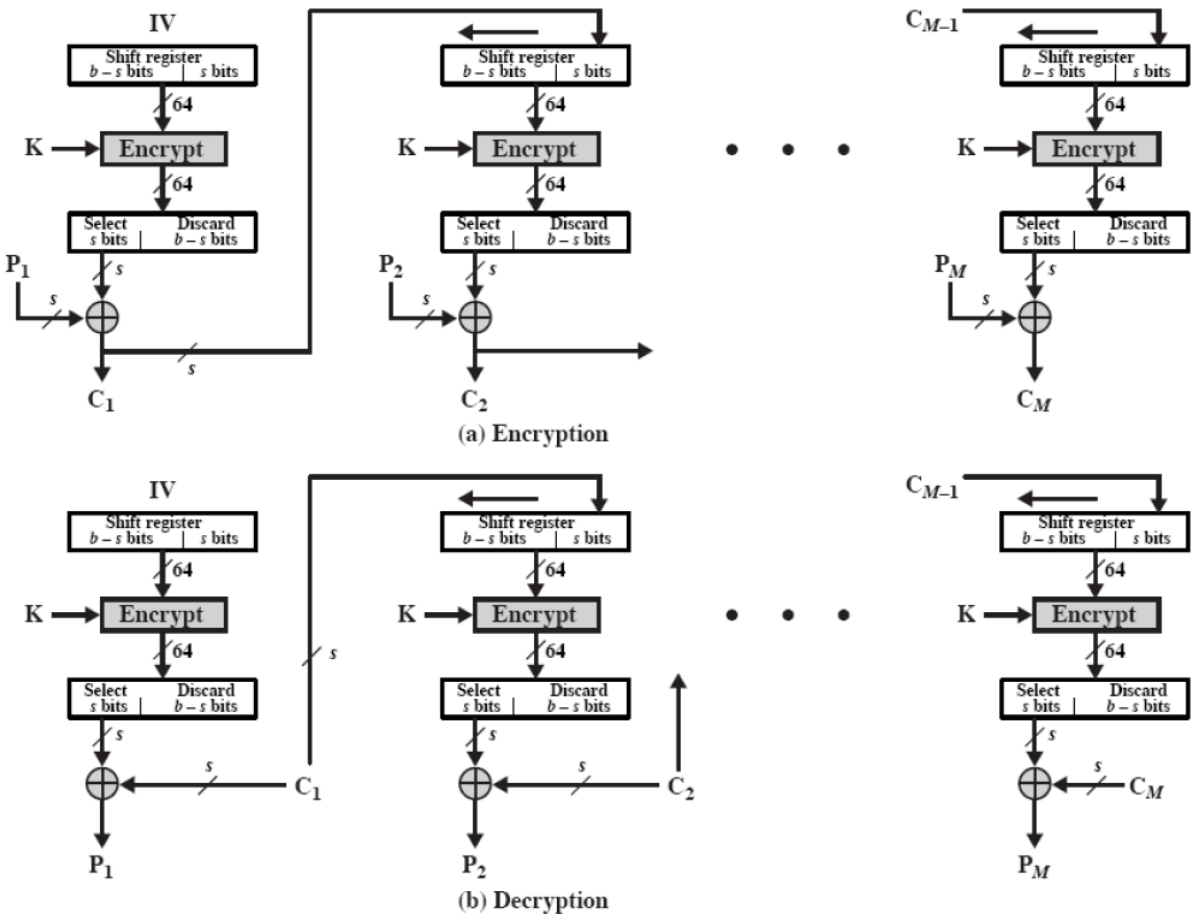
-both parties should agree on an IV

Cipher FeedBack (CFB)

-Message is treated as a stream of bits

-Internet için kullanılabilir veya voice encryption

--C1 bi tane bit buna birşey olursa p1 hatalı olur aynı zamanda feedback de olduğu için p2 yi de etkile oda bozuk çıkar taki p64 e kadar çünkü en sağdan giriyo c1 64 bitlik shift register her seferinde bir bit sola kayıyor.64 bit sonra çıkacak yanlış bit ve diğer plaintextlerde sorun olmicak.



Output FeedBack (OFB)

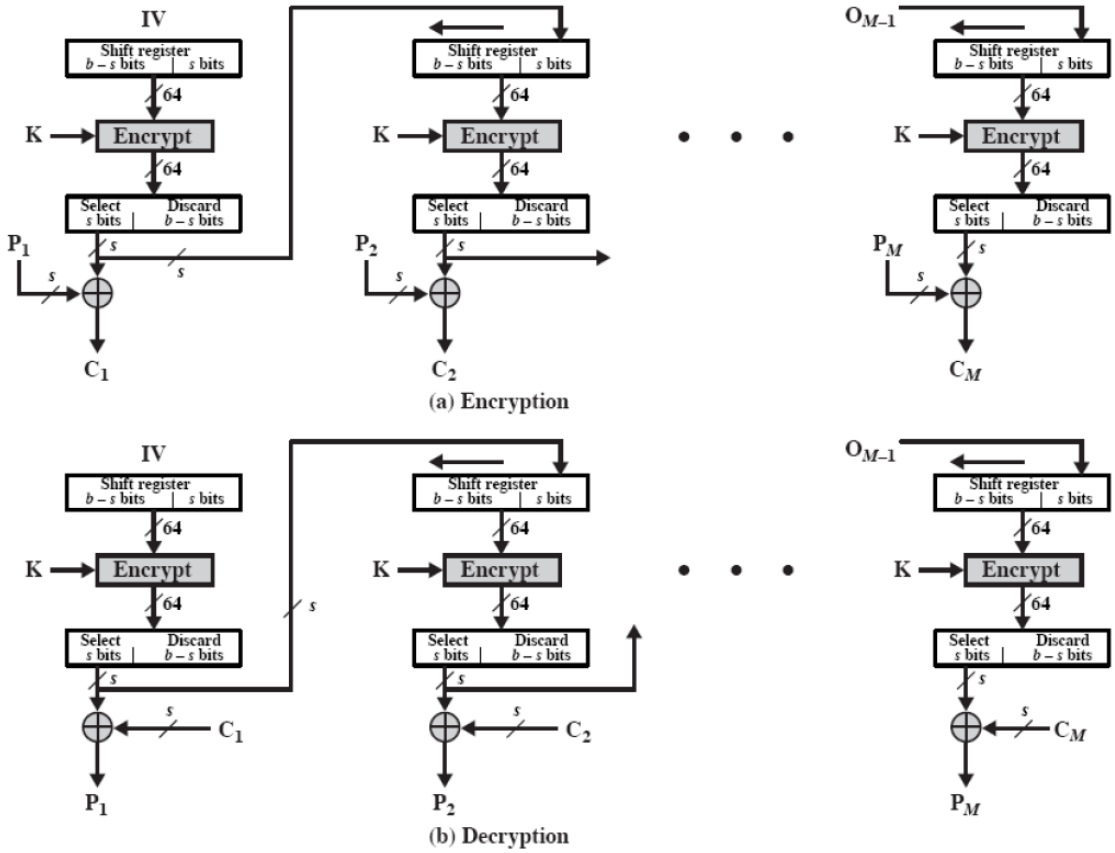
-another stream mode

-feedback is independent of transmission, so transmission errors do not propagate

-same IV should not be used twice for the same key (general problem of using IV)

otherwise, when two cipher text block s are XORed
the random sequence is cancelled and the
attacker has obtains XOR of two plaintexts

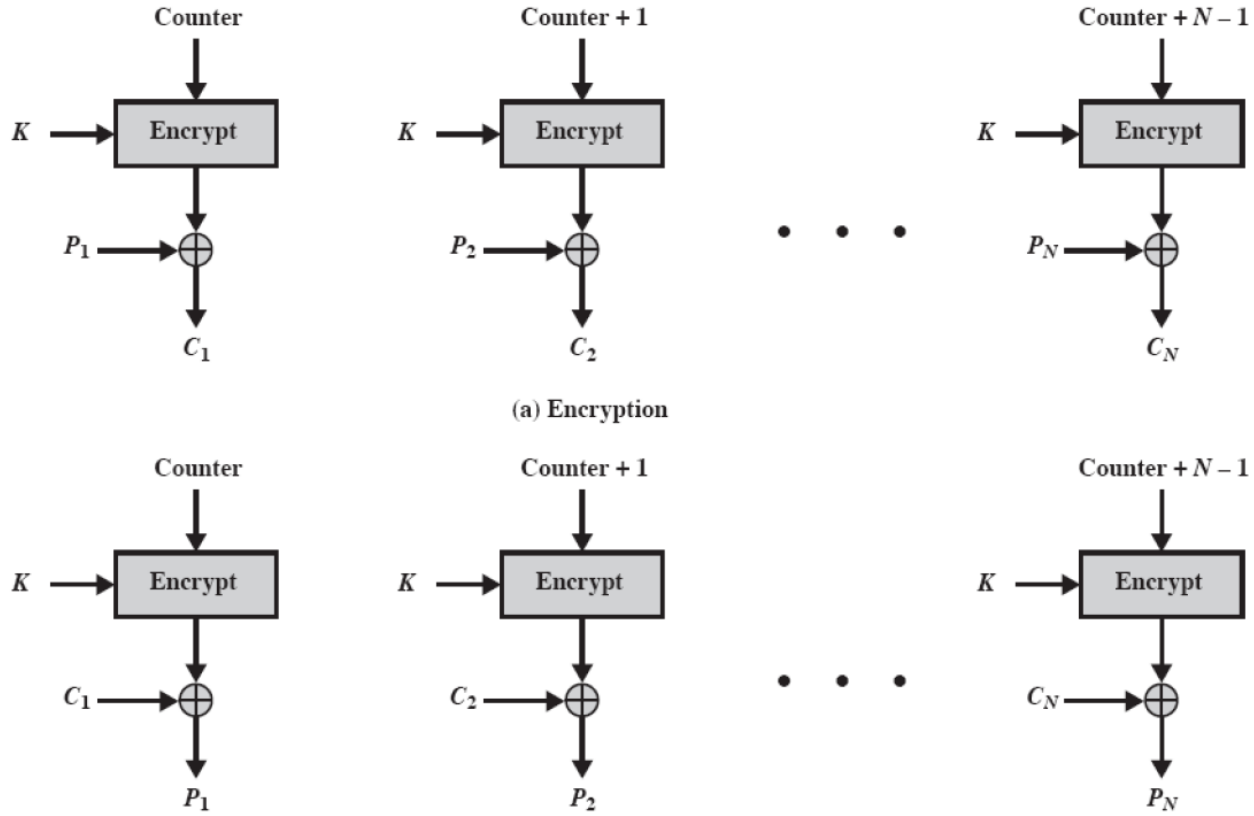
Output FeedBack (OFB)



-C1 ye bişey olursa P1 de error olur.ama diğer bitlerde problem çıkmaz üstteki sorunu çözmüş olur.

Counter(CTR)

-For the same key, the counter value should not repeat



Preprocessing: the encryption part can be done offline and when the message is known, just do the XOR.
Random Access: decryption of a block can be done in random order, very useful for hard-disk encryption.

Parallel Encryption : efficient can do parallel encryptions

Messages of Arbitrary Length: ciphertext is the same length with the plaintext (i.e., no IV).