Computer security – protection offered to automated system to preserve confidentiality , integrity and availability

Network Security – set of rules and configuration used to preserve confidentiality , integrity and availability of a network

Vulnerability – weakness in system

Attack – human will exploit vulnerability of system to gain access to system resources

Threat – set of circumstances that can lead to potential loss in system

Security Goals – Confidentiality , Integrity , Availability , Authentication , Non repudiation

Passive attack – no resource alteration , hard to detect

Eg – traffic analysis and eavesdropping , snooping

Active attack – resource alteration , easy to detect using appropriate mechanism

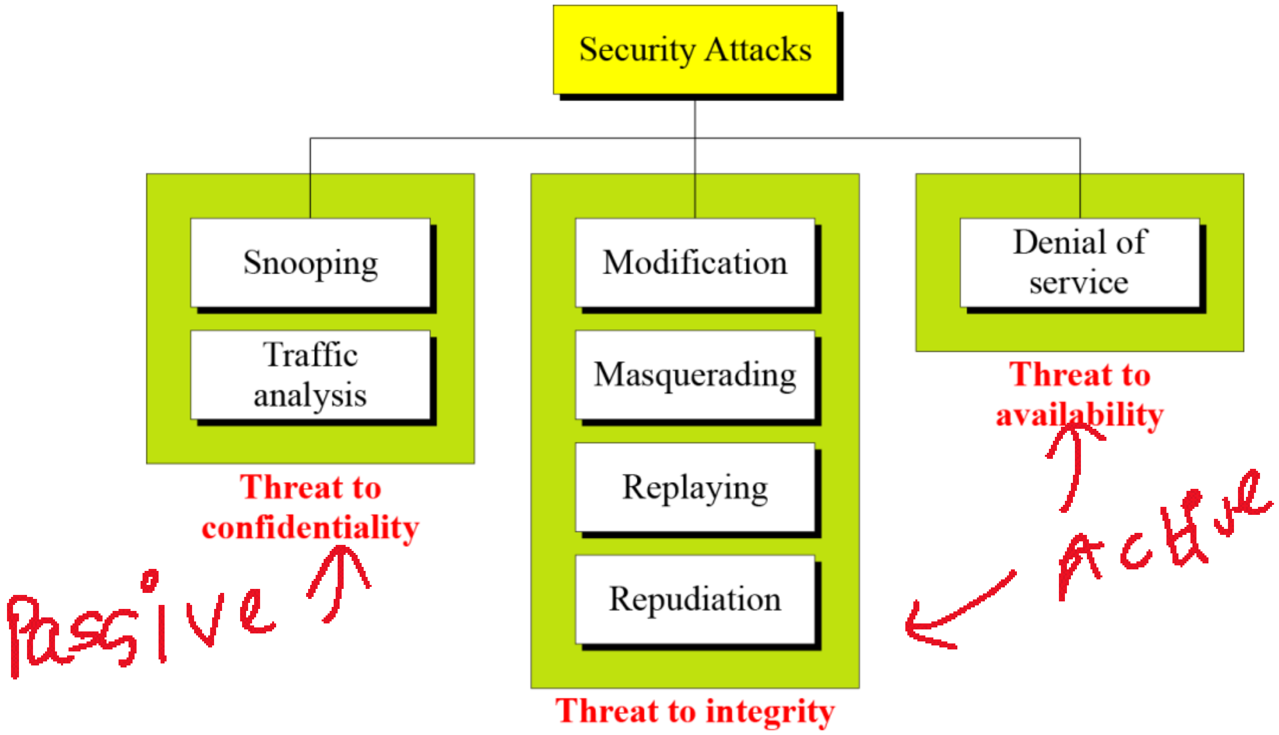
Eg – Masquerade , replay , DOS

Snooping – unauthorised access to data

Traffic analysis – traffic monitoring

Masquerade – one entity pretends to be other to gain access to data

Replay – capture the data unit , retransmit it to produce unauthorised access



Cryptology – art of making and breaking secret code

Cryptography – making secret code

Cryptanalysis – breaking secret code

Plaintext – orignal message

Ciphertext – encrypted message

Cipher – making ciphertext

Symmetric Encryption – same key for encryption and decryption , fast , key exchange is problem , length of cipher text is nearly same as plain text ,

N(N-1)/2 keys for N participants , only encryption and decryption can be done (confedentiality) , not used for digital signature (integrity , repudiation)

Assymetric Encryption – different key for encryption and decryption , slow , key exchange is not a problem , length of cipher text is more than plain text ,

N keys for N users , used for both confedentaility and integrity/repudiation hence for digital signature

Stream cipher – faster as individual encryption is done , low error propogation , no diffusion as each symbol is seperately encrypted , attacker can insert suspicious symbol due to individual encoding

Block cipher – slower as one block is encrypted , more error propogation , diffusion is evident , attacker cannot insert suspicious symbol

Confusion – if one bit of key is modified , most of cipher text bits will also be modified , both stream and block cipher use confusion , relation between cipher text and key is masked by confusion

Diffusion – if one bit in plain text is modified then most of cipher text bits are modified , only used by block cipher , relation between cipher text and plain text is masked by diffusion

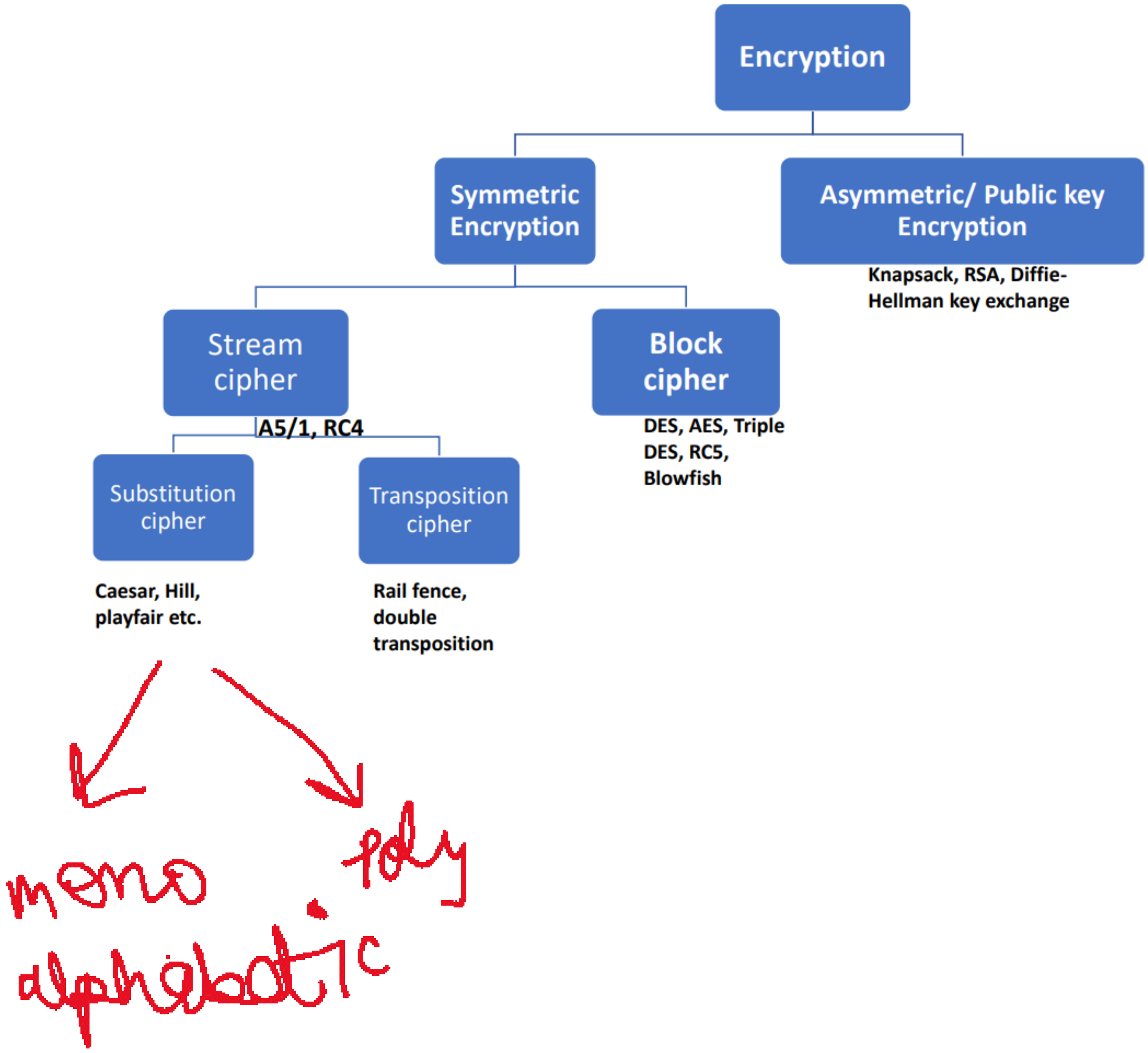
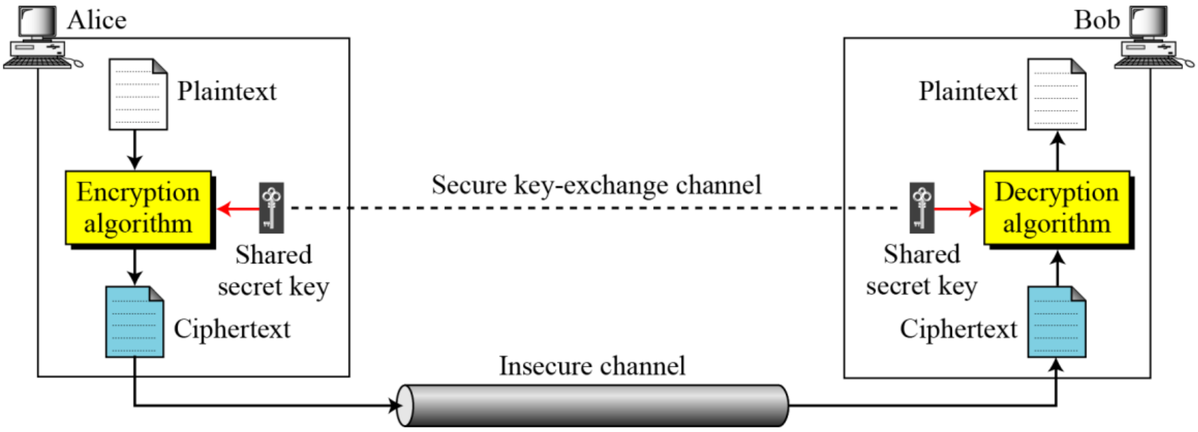

Encryption
Symmetric Encryption
Asymmetric/ Public key Encryption
Knapsack, RSA, Diffie-Hellman key exchange
Stream cipher
A5/1, RC4
Block cipher
DES, AES, Triple DES, RC5, Blowfish
Substitution cipher
Transposition cipher
Caesar, Hill, playfair etc.
Rail fence, double transposition
mono alphabetic
poly

Figure: General idea of symmetric-key cipher



Asymmetric Key Cryptography

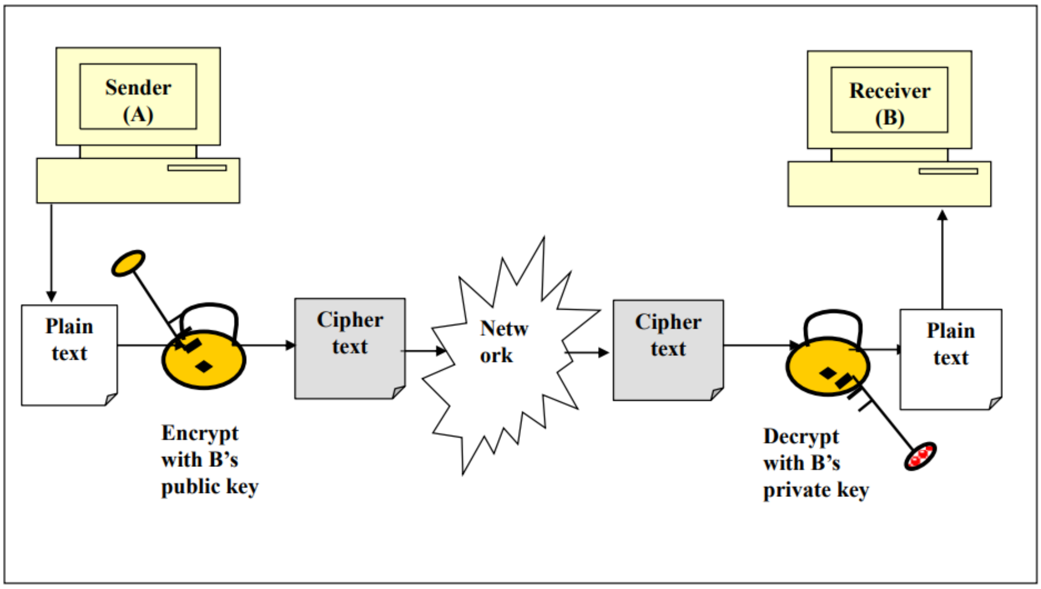
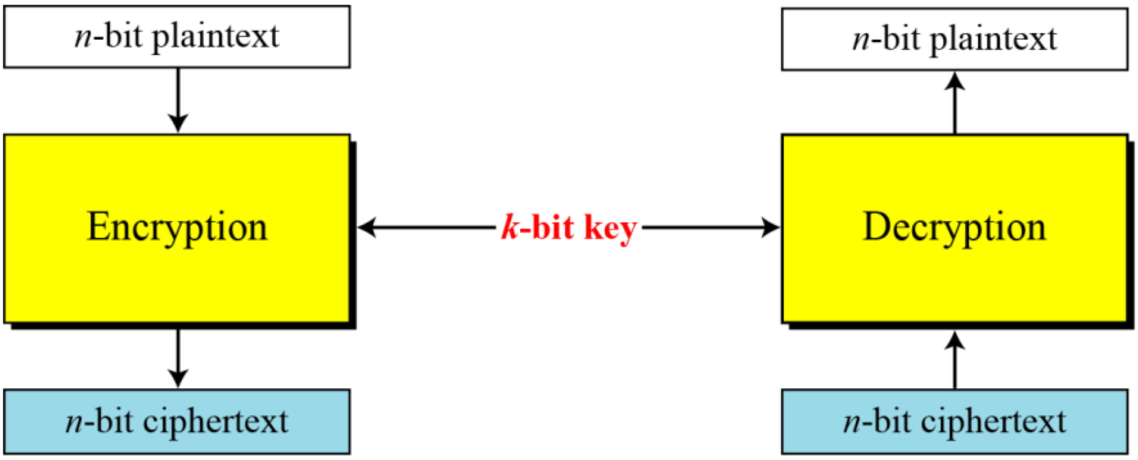


Figure: *A modern block cipher*



Kerchoff principle - The principle states that a cryptographic system should remain secure even if everything about the system, except the key, is public knowledge.

Monoalphabetic substitution – one to one relation between plaintext and ciphertext

Polyalphabetic substitution – one to many relation between plaintext and ciphertext

Historically, additive ciphers are called shift ciphers. Julius Caesar used an additive cipher to communicate with his officers. For this reason, additive ciphers are sometimes referred to as the **Caesar cipher. Caesar used a key of 3 for his communications.**

Breaking shift cipher – brute force , frequency analysis

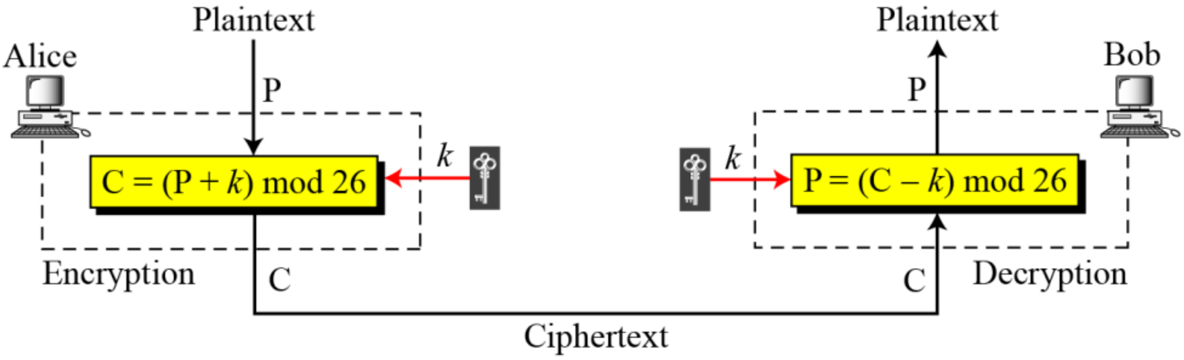
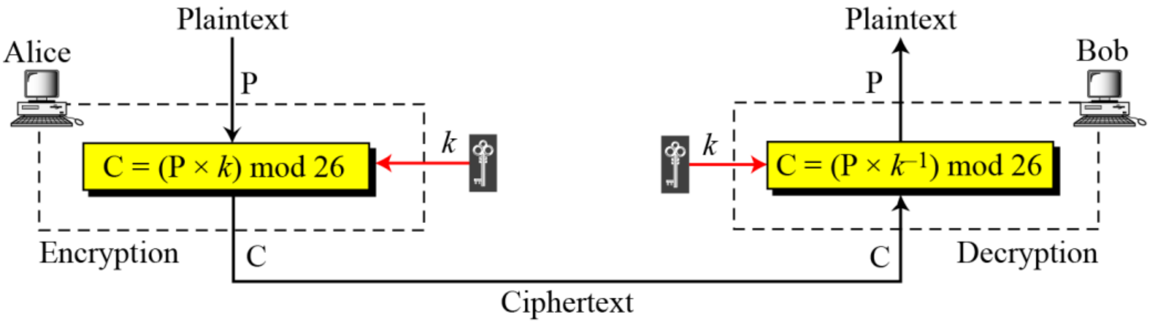


Figure 3.10 ***Multiplicative cipher***



16|08|23

CNS Numericals

i) Shift Cipher (keyspace = 26!) ~~Bruteforce~~ Frequency Analysis

· encryption (p+k) % 26 | monoalphabetic |

decryption (c-k) % 26

· caesor cipher, shift cipher with k=3

eg] encode "hello" k=15

→

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16

r	s	t	u	v	w	x	y	z
17	18	19	20	21	22	23	24	25

h → 07 Encryption → (07+15)%26 → 22 (W)

e → 04 (04+15)%26 → 19 (T)

l → 11 (11+15)%26 → 0 (A)

l → 11 (11+15)%26 → 0 (A)

o → 14 (14+15)%26 → 3 (D)

ii) PlayfairCipher (polyalphabetic) keyspace = 25!

attack → joson plain text, joson cipher text

· Rules :

i) Before encrypting plain text if two consecutive letter in plain text are same then insert bogus char. 'x' in between them

ii] If both character are in same row replace them by immediate right character from same row

iii) If two character appear in same column replace them with immediate bottom character

iv) If above cases are not satisfied then replace character by character in same row but in column of other character.

16/08/23

Page No. 01

Date: 16/08/23

Eg] Plaintext : hello

key : security

Boguschar (R1)

→ plaintext : he lx lo

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

5x5 matrix

Plaintext : he lx lo

ciphertext : fu oq mp

(R4) (R4) (R2)

Eg] plaintext : niranjan

Key : network security

→ plaintext : ni ra nj an

rf si rf it

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

iii) Vigenere cipher (keyspace : 26^n, kasiki, freq analysis)

length of key

Eg] plaintext : life is full of surprises

key : health

a b c d e f g h i j k l m n o p

0 1 2 3 … 10 11 12 13 14 15

q r s t

16 17 18 19 20 21 22 23 24 25

· divide plaintext into group of n → length of key

life is   full of   surpri   ses

[plain] → A → 11, 8, 5, 4, 8, 18   5, 20, 11, 11, 14, 5   18, 20, 17, 15, 17, 8   18, 4, 18

[key] → health   health   health   hea

B → 7, 4, 0, 11, 19, 7   7, 4, 0, 11, 19, 7   7, 4, 0, 11, 19, 7   7, 4, 0

· monoalphabetic substitution:

(P+C)%26 → (A+C)%26.

(18%26), (12%26), (5%26)
(15%26), (27%26), (25%26)

→ 8, 12, 5, 15, 1, 25

(12%26), (24%26), (11%26)
(22%26), (33%26), (12%26)

→ 12, 24, 11, 22, 7, 12

(25%26), (24%26), (17%26)
(26%26), (36%26), (15%26)

→ 25, 24, 17, 0, 10, 15

(25%26), (8%26), (18%26)

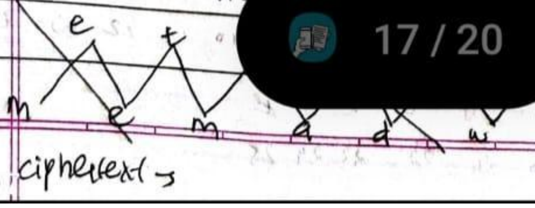
→ 25, 8, 18

ciphertext → imfpbz   mylwhm   zyrakp   zis

~~iv) Railfence cipher (transposition)~~

~~· keyspace → n (no. of rows), attack → Brute force~~

~~Eg) Plaintext: me~~



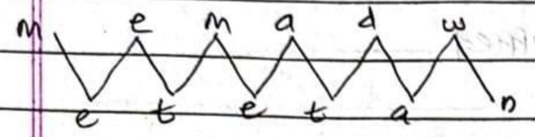
ciphertext →

iv) Raifence cipher (transposition) keyless

- keyspace → n (no of rows), attack → brute force

Eg)

- plaintext → meet me at dawn



- ciphertext → memadw etetan

$\underbrace{\text{memadw}}_{R1}$ $\underbrace{\text{etetan}}_{R2}$

v) columnar cipher (transposition) keyless

- plaintext: meet me at dawn

no of column → 4

$$\begin{bmatrix} m & e & e & t \\ m & e & a & t \\ d & a & w & n \end{bmatrix}$$

- letters → 12, column → 4
- Row → 12/4 → 3

- ciphertext → mmd eea eaw ttn

vi) single transposition (keyed)

- sender/receiver aggree on common number in which plaintext is divided

Eg) plaintext: meet me at dawn

Group of 4

plaintext: meet meat dawn

key → [2 4 1 3] → encryption

ciphertext: e t [illegible] endw

16/08/23 · insert bogus character if needed

- decryption (key)

senderkey $\begin{array}{|c|c|c|c|} \hline 2 & 4 & 1 & 3 \\ \hline \end{array}$ → $\begin{array}{|c|c|c|c|} \hline 1 & 2 & 3 & 4 \\ \hline \end{array}$ → $\begin{array}{|c|c|c|c} \hline 3 & 1 & 4 & 2 \\ \hline \end{array}$

$\begin{array}{cccc} 1 & 2 & 3 & 4 \end{array}$ $\qquad$ $\begin{array}{cccc} 2 & 4 & 1 & 3 \end{array}$

- only columns are shuffled

vii) Double transposition

- Both row and column are shuffled

Eg] plaintext : meet me at dawn

a) create matrix by seeing total letters:

total: 12 (4×3)

$$\begin{array}{c|ccc|} R/C & 1 & 2 & 3 \\ 1 & m & e & e \\ 2 & t & m & e \\ 3 & a & t & d \\ 4 & a & w & n \end{array}$$

b) shuffle Row :

[1 2 3 4) ⇒ [2, 4, 1 3]

$$\begin{bmatrix} a & t & d \\ m & e & e \\ a & w & n \\ t & m & e \end{bmatrix}$$

c) shuffle column:

[1 2 3] → [2 3 1]

$$\begin{bmatrix} d & a & t \\ e & m & e \\ n & a & w \\ e & t & m \end{bmatrix}$$

- Read above matrix row wise:

dat eme naw etm

16/08/23

confedentiality → public key of receiver (encryp), private key of receiver (decryp)

authen,

non repudiation → private key of sender (encrypt)

decryption:

i) create matrix (4 row, 3 column)

$$\begin{bmatrix} d & a & t \\ e & m & e \\ n & a & w \\ e & t & m \end{bmatrix}$$

column permutation

$$\begin{array}{|c|c|c|} \hline 2 & 3 & 1 \\ \hline \end{array} \rightarrow \begin{array}{|c|c|c|} \hline 1 & 2 & 3 \\ \hline \end{array} \rightarrow \begin{array}{|c|c|c|} \hline 3 & 1 & 2 \\ \hline \end{array}$$

$$\begin{array}{ccc} 1 & 2 & 3 \end{array} \qquad \begin{array}{ccc} 2 & 3 & 1 \end{array} \qquad \begin{array}{ccc} 1 & 2 & 3 \end{array}$$

$$\begin{bmatrix} a & t & d \\ m & e & e \\ a & w & n \\ t & m & e \end{bmatrix} \leftarrow$$

$[1, 2, 3] \rightarrow [3, 1, 2]$.

ii) row permutation sequence :

$$\begin{array}{|c|c|c|c|} \hline 2 & 4 & 1 & 3 \\ \hline \end{array} \rightarrow \begin{array}{|c|c|c|c|} \hline 1 & 2 & 3 & 4 \\ \hline \end{array} \rightarrow \begin{array}{|c|c|c|c|} \hline 3 & 1 & 4 & 2 \\ \hline \end{array}$$

$$\begin{array}{cccc} 1 & 2 & 3 & 4 \end{array} \qquad \begin{array}{cccc} 2 & 4 & 1 & 3 \end{array} \qquad \begin{array}{cccc} 1 & 2 & 3 & 4 \end{array}$$

$[1, 2, 3, 4] \rightarrow [3, 1, 4, 2]$

$$\begin{bmatrix} m & e & e \\ t & m & e \\ a & t & d \\ a & w & n \end{bmatrix}$$

∴ meet meat dawn

viii) **RSA**

i) Find p, q, (p and q are large prime nos) $p \neq q$

ii) $n \leftarrow p \times q$

iii) $\phi(n) \leftarrow (p-1) * (q-1)$

iv) select key (e) such that $1 < e < \phi(n)$ and $\gcd(e, \phi(n)) = 1$

v) $d \leftarrow e^{-1} \% \phi(n)$ i.e. $\boxed{d = \frac{k\,\phi(n) + 1}{e}}$

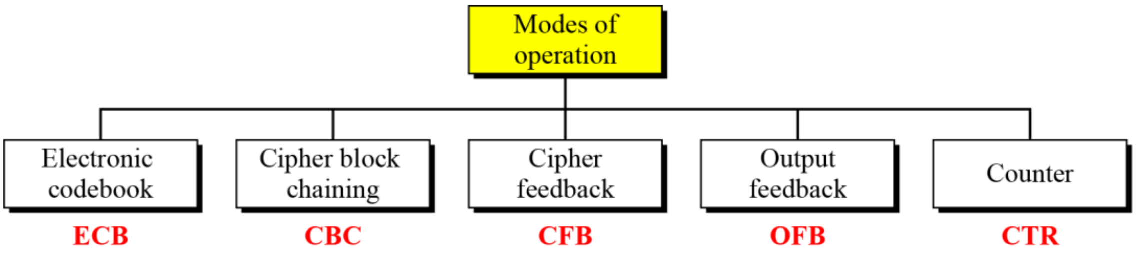
↑ select k such that d is integer

∴ $\boxed{\begin{array}{l} \text{publickey} \rightarrow (e, n) \\ \text{privatekey} \rightarrow d \end{array}}$

$\boxed{\text{encryption} \rightarrow m^{e} \% n}$ $\boxed{\text{decryption} \rightarrow c^{d} \% n}$

The most common public-key algorithm is the RSAcryptosystem, named for its inventors (Rivest, Shamir, and Adleman)

Figure 8.1 ***Modes of operation***



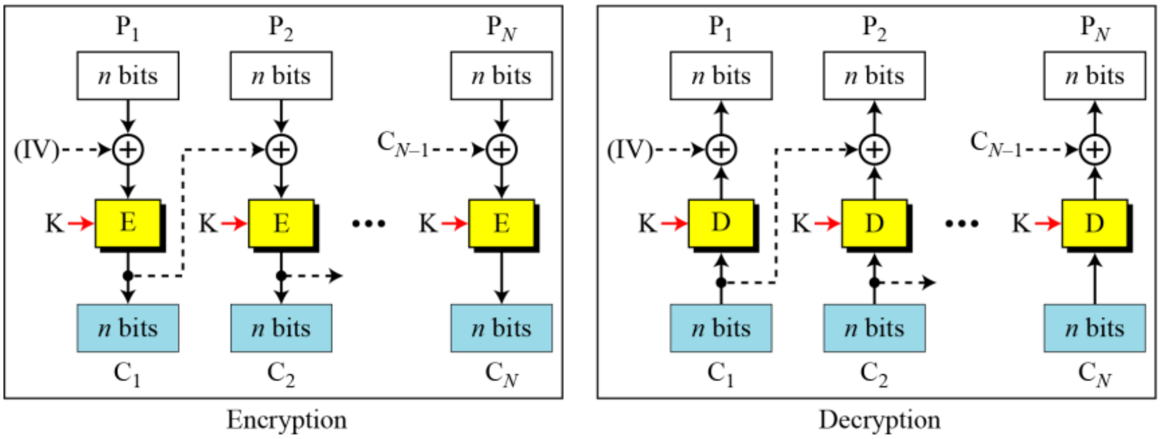
Block

8.1.2 Cipher Block Chaining (CBC) Mode

In CBC mode, each plaintext block is exclusive-ored with the previous ciphertext block before being encrypted.

Figure 8.3 *Cipher block chaining (CBC) mode*

E: Encryption	D : Decryption
P_i: Plaintext block *i*	C_i : Ciphertext block *i*
K: Secret key	IV: Initial vector (C_0)

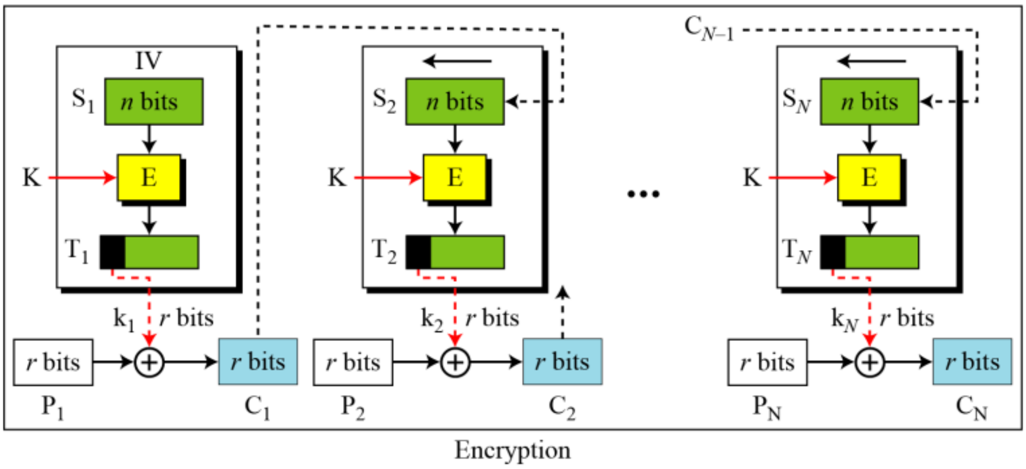


8.1.3 Cipher Feedback (CFB) Mode

In some situations, we need to use DES or AES as secure ciphers, but the plaintext or ciphertext block sizes are to be smaller.

Figure 8.4 *Encryption in cipher feedback (CFB) mode*

E : Encryption	D : Decryption	S_i: Shift register
P_i: Plaintext block *i*	C_i: Ciphertext block *i*	T_i: Temporary register
K: Secret key	IV: Initial vector (S_1)	



stream

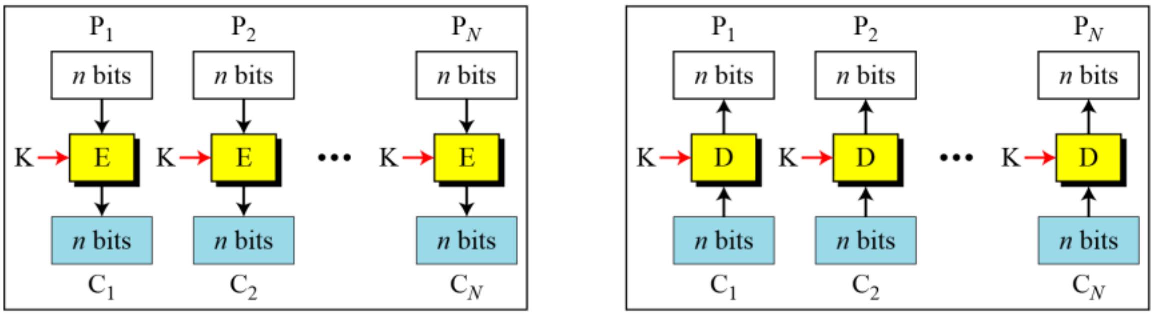
8.1.1 Electronic Codebook (ECB) Mode

The simplest mode of operation is called the electronic codebook (ECB) mode.

Encryption: $C_i = E_K(P_i)$ Decryption: $P_i = D_K(C_i)$

Figure 8.2 ***Electronic codebook (ECB) mode***

E: Encryption D: Decryption
P_i: Plaintext block *i* C_i: Ciphertext block *i*
K: Secret key



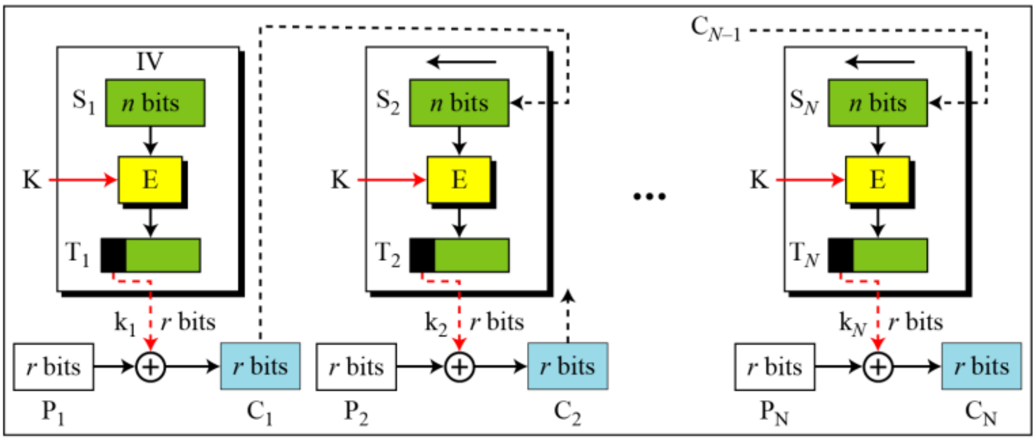
Encryption Decryption

8.1.3 Cipher Feedback (CFB) Mode

In some situations, we need to use DES or AES as secure ciphers, but the plaintext or ciphertext block sizes are to be smaller.

Figure 8.4 ***Encryption in cipher feedback (CFB) mode***

E : Encryption D : Decryption S_i: Shift register
P_i: Plaintext block *i* C_i: Ciphertext block *i* T_i: Temporary register
K: Secret key IV: Initial vector (S_1)



Encryption

18.1.4 Output Feedback (OFB) Mode

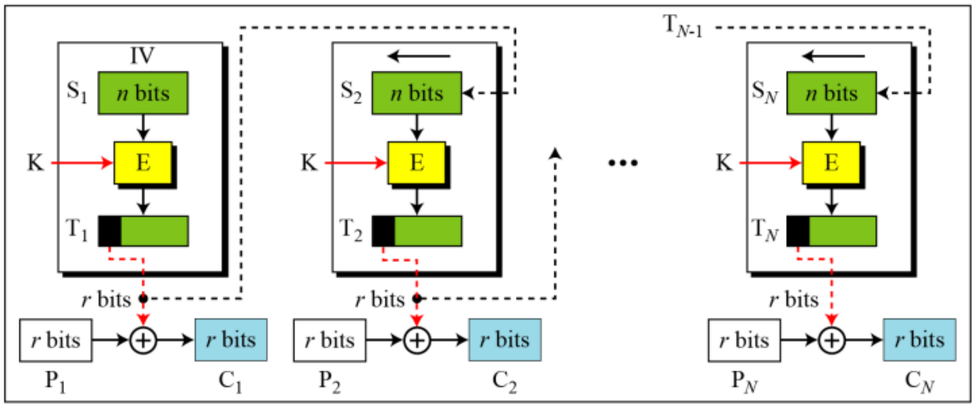
In this mode each bit in the ciphertext is independent of the previous bit or bits. This avoids error propagation.

Figure 8.6 ***Encryption in output feedback (OFB) mode***

E : Encryption
P_i: Plaintext block i
K: Secret key

D : Decryption
C_i: Ciphertext block i
IV: Initial vector (S_1)

S_i: Shift register
T_i: Temporary register



Encryption

8.1.5 Counter (CTR) Mode

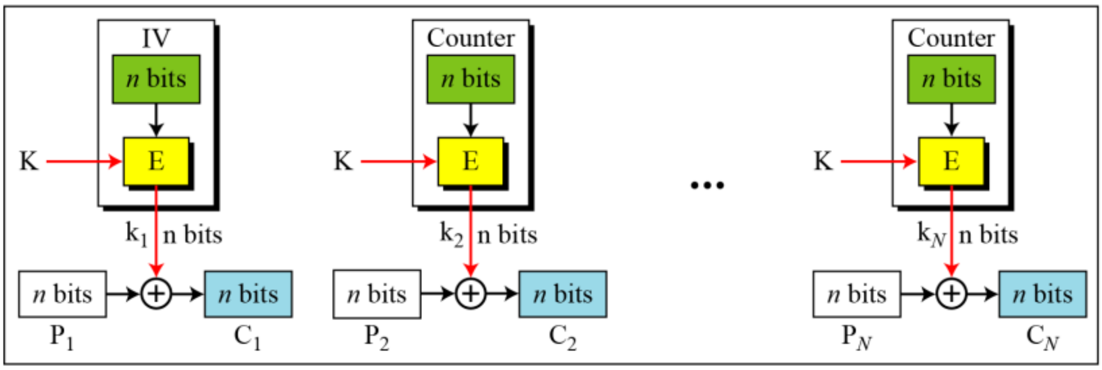
In the counter (CTR) mode, there is no feedback. The pseudorandomness in the key stream is achieved using a counter.

Figure 8.8 ***Encryption in counter (CTR) mode***

E : Encryption
P_i: Plaintext block *i*
K : Secret key

IV: Initialization vector
C_i: Ciphertext block *i*
k_i : Encryption key *i*

The counter is incremented for each block.



Encryption

Symmetric-key cryptography is more efficient than asymmetric-key cryptography for enciphering large messages. Symmetric-key cryptography

A KDC creates a secret key for each member. This secret key can be used only between the member and the KDC, not between two members.

KDC protocol – Needham-Schroedar Protocol , Otway Rees protocol

Kerberos is an authentication protocol, and at the same time a KDC, that has become very popular. Several systems, including Windows 2000, use Kerberos. Originally designed at MIT, it has gone through several versions

Components of Kerberos –

Authentication Server (AS) – KDC in kerberos protocol

Ticket-Granting Server (TGS) - The ticket-granting server (TGS) issues a ticket for the real server (Bob).

Real Server - The real server (Bob) provides services for the user (Alice)

Symmetric Key aggrement –

Diffe Hellman – discrete logarithmic attack , man in middle attack

Station-to-Station

Shannon introduced the concept of a product cipher. A product cipher is a complex cipher combining substitution, permutation, and other components

Product cipher – fiestal cipher , non fiestal cipher

DES – symmetric key block cipher published by NIST (national institute of standard and technology)

DES – initial permutation + 16 rounds + final permutation

Avalanche Effect – small change in plaintext create significant change in ciphertext

Completeness Effect – each bit of ciphertext need to depend on as many bits as plaintext

Figure 6.1 *Encryption and decryption with DES*

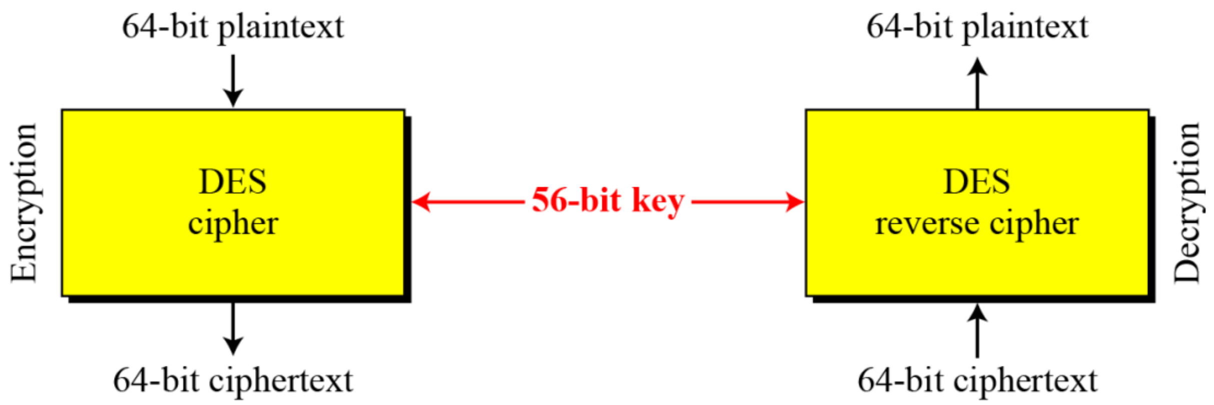
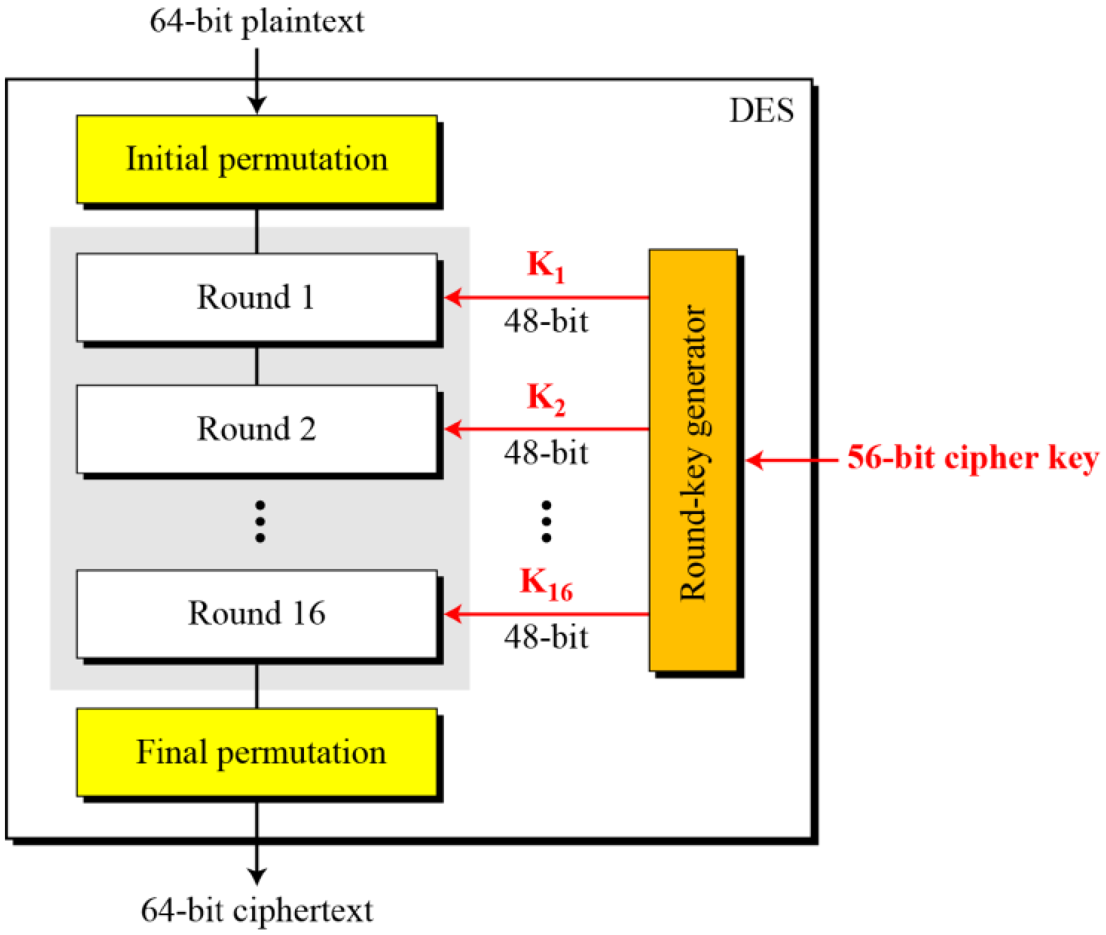


Figure 6.2 *General structure of DES*



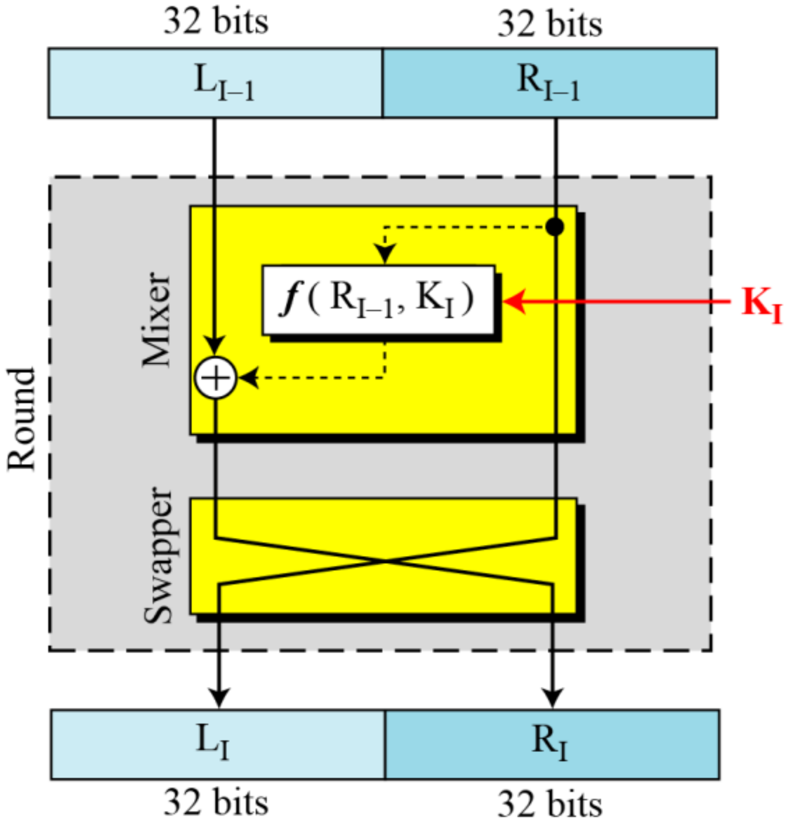


Figure 6.4

A round in DES (encryption site)

32-bit output.

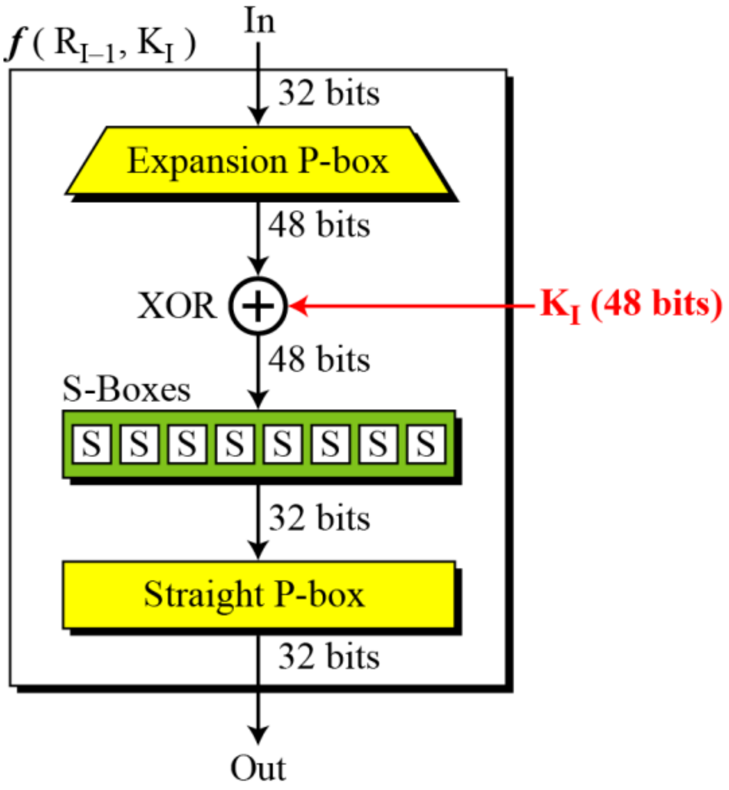


Figure 6.5

DES function

Double DES suffer from man in middle attack , hence triple DES is used , like in PGP

Expansion PBox convert 32bit to 48bit , 8 **SBoxes** used in DES they do real mixing 48bit to 32bit

SSL is used to establish link between web server and browser , works in transport layer

SSL services –

- Fragmentation - SSL divides data into blocks of 214 bytes or less
- Compression – compresses each block of data using lossless compression
- Message Integrity – uses keyed hash function to create MAC
- Confidentiality – original data and MAC are encrypted using symmetric key cryptography
- Framing – A header is added to encrypted payload and then payload is passed to transport layer protocol

SSL Handshake –

1) **Information exchange –**
   Client – version , client random no , session ID , cipher suite , compression methods
   Server – version , server random no , session ID , selected cipher suite , selected compression method
2) **Server Identification and Key Exchange –**
   Sever to client – chain of ceertificate , server public key
3) **Client Identification and Key Exchange –**
   Client to server – chain of certificate , client public key
4) **Final handshake**
   Client to server – change cipher spec value , md5+sha hash
   Server to client - change cipher spec value , md5+sha hash

IPSec – network layer , complex

SSL – transport layer , simple

IPSec, or Internet Protocol Security, is a widely used protocol suite that helps secure Internet Protocol (IP) communications by authenticating and encrypting each IP packet in a data stream. It is commonly used for establishing secure virtual private networks (VPNs) over the internet. IPSec provides data confidentiality, integrity, and authentication, making it a valuable tool for ensuring secure communication between networks, especially over untrusted or public networks like the internet.

PGP - Pretty Good Privacy (PGP) is a security program used to decrypt and encrypt email and authenticate email messages through digital signatures and file encryption. PGP was first designed and developed in 1991 by Paul Zimmerman, a political activist.

PGP follows a three-step process:

Step 1: PGP generates a huge, one-time-use public encryption algorithm that cannot be guessed, which becomes the random session key.

Step 2: The session key is then encrypted using the recipient's public key, which protects the message while being transmitted. The recipient shares that key with anyone they want to receive messages from.

Step 3: The message sender submits their session key, then the recipient can decrypt the message using their private key.

Public key versions of PGP – RSA , Diffie Hellman

IPSec – suite of protocol to secure communication over internet , can operate in two modes tunnel mode and transport mode

Transport mode – IPSec secure payload , header is untouched , used in end to end comm like host to host and host to gateway comm

Tunnel mode – New IP header is used as a cover hence both payload and header are protected , used in communication between two network or two gateway

IDS – security mechanism to detect and moniter unautorised access and malicious activity , identify potential threat like hacking attempt , attack etc

IDS approach – Signature based , anomaly based

IDS architecture – NIDS , HIDS

NIDS – moniter network and detect unusual pattern

HIDS – installed on individual host system , moniter activity , system log , file integrity

Signature based – known attack signature and current are matched , cannot predict zero day attacks

Anomaly based – threshold is estabished , if crossed alert is raised , can prevent zero day attacks

Firewall – main component of NAC , moniter incoming and outgoing traffic

Types –

A) **PacketFilter** – operate in network layer , filter source IP , destination IP , source port , destination port
If attacker send TCP packet with ack , then packet filter will not reject it and port can be tampered

B) **Stateful Packet Filter** – contain state and hence can remember history , works in transport layer

C) **Application proxy** – attacker must convince proxy if data is safe to allow data to enter system

D) **Personal firewall**

SSL and TLS both work in network layer , but in TLS generation of cryptographic function is more complex and involves data expansion function and pseudorandom function

Malware – malicious software that damage or disable computer system and gives limited/full access of system to malware creator , Eg – virus , worm , trojan , rootkit , backdoor , botnet , ransomware , spyware , adware etc

Virus – attach to other program to propogate , can be transient(ends with host) and resident(finds place in memory)

They can live inside program , memory . boot etc

4 phases – dormant (idle , virus can be activated by an event) , propogation(make copies) , triggering(do intended work) , execute(perform function)

SPAM – unwanted , unsolicited communication that gets sent over bulk

Eg – phishing mail , email spoofing , tech support scam , current event scam

Trojan – program in which harmful code is present inside a legitimate code and has same privileges as victim

Indications – DVD tray open , wallpaper change auto , printer auto , screen blick etc

Ways of transmission – software , popup ads , email attachment etc

Phishing – deceiving user to share secret info , user requesting info look like legitimnate user but is attacker

Types – Email phishing , spear phishing(target group of individuals) , vishing, smishing , clone phishing(actual mail is modified)

Keylogger – spyware to store info about consecutiv key strokes , not always illegal, used in IT industry

Types – software (form grabbing,JavaScript,API) , hardware(device based)

Transmission – webpage script , phishing , social engineering

Observation – laggy mouse , slow browser , disappearing cursor

DOS attack types – PING flood , SYN flood , UDP flood , HTTP flood , DNS amplification (exploit DNS resolver) , NTP amplification

A **backdoor attack** is a secret method of avoiding normal authentication procedures to gain unauthorized access to a system.A backdoor attack can result in privilege escalation, lateral movements

Simple Network Management Protocol (SNMP) is an Internet Standard protocol

• for collecting and organizing information about managed devices on IP networks and

• for modifying that information to change device behavior.

- Devices that support SNMP include cable modems, routers, switches, servers, workstations, printers, and more.

Components – management station(collect info from network by regurarly checking for updates) , agent(poll information and send it to management station)

NAC - manage access to network , decide which user can log in and what can they acces

Components – Access Requestor , Policy Server , NAS(network access server)

NAS is media gateway

NAC enforcement methods – IEEE 802.1X (link layer protocol that ensures authorization before port is assigned) , Firewall , DHCP (allocate dynamic IP address to host) , VLAN

HTTP - 80 , HTTPS – 443

The following elements of the communication are encrypted:

- URL of the requested document
- Contents of the document
- Contents of browser forms (filled in by browser user)
- Cookies sent from browser to server and from server to browser
- Contents of HTTP header

Shift cipher can have 26 key combinations , hence it can be easily broken down using brute force atack in which attcaker will try out every possible combination until plaintext is obtained , shift should be known

Keyspace – 26

Monoalphabetic cipher , example is caesar cipher , hence it cannot be broken down with help of brute force , frequency analysis needs to be used . Keyspace is **26!**

In frequency analysis , a predefined table is present for plaintext and the frequncy table obtained is compared with predefined table , then frequency is compared and if it matches with frequency in plaintext table then it is mapped .

Vigenere cipher – polyalphabetic substitution cipher

Eg - Plaintext :- hello world

Key:- vig

Hel low orl d

Vig vig vig v
(p+c)%26

Where p ~ H and c~V

Ciphertext – **cmrgwcjzry**

Keyspace – 26^n . n is length of key

The Kasiski test is a cryptanalytic method for breaking the Vigenere cipher. It works by looking for repeated sequences of characters in the ciphertext. If a repeated sequence of characters is found, the distance between the occurrences of the sequence is likely to be a multiple of the length of the keyword.

Cryptanalysis on the Playfair cipher involves attempting to break the encryption without knowing the key or the plaintext-ciphertext pair. Most common way is using frequency analysis

Keyspace of playfair cipher – ways to arrange mxn elements , i.e. apx 10^(mxn) , mxn is size of matrix

Keyspace of vigenere cipher – 26^n . n is length of key

Key features of AES:

1)Type of cipher: Symmetric-key block cipher

2)Number of rounds: 10, 12, or 14 rounds, depending on the key size

3)Keysize: 128, 192, or 256 bits

4)Block size: 128 bits

5)Operations in each round:

Byte substitution (SubBytes)

Shift rows (ShiftRows)

Mix columns (MixColumns)

Add round key (AddRoundKey)

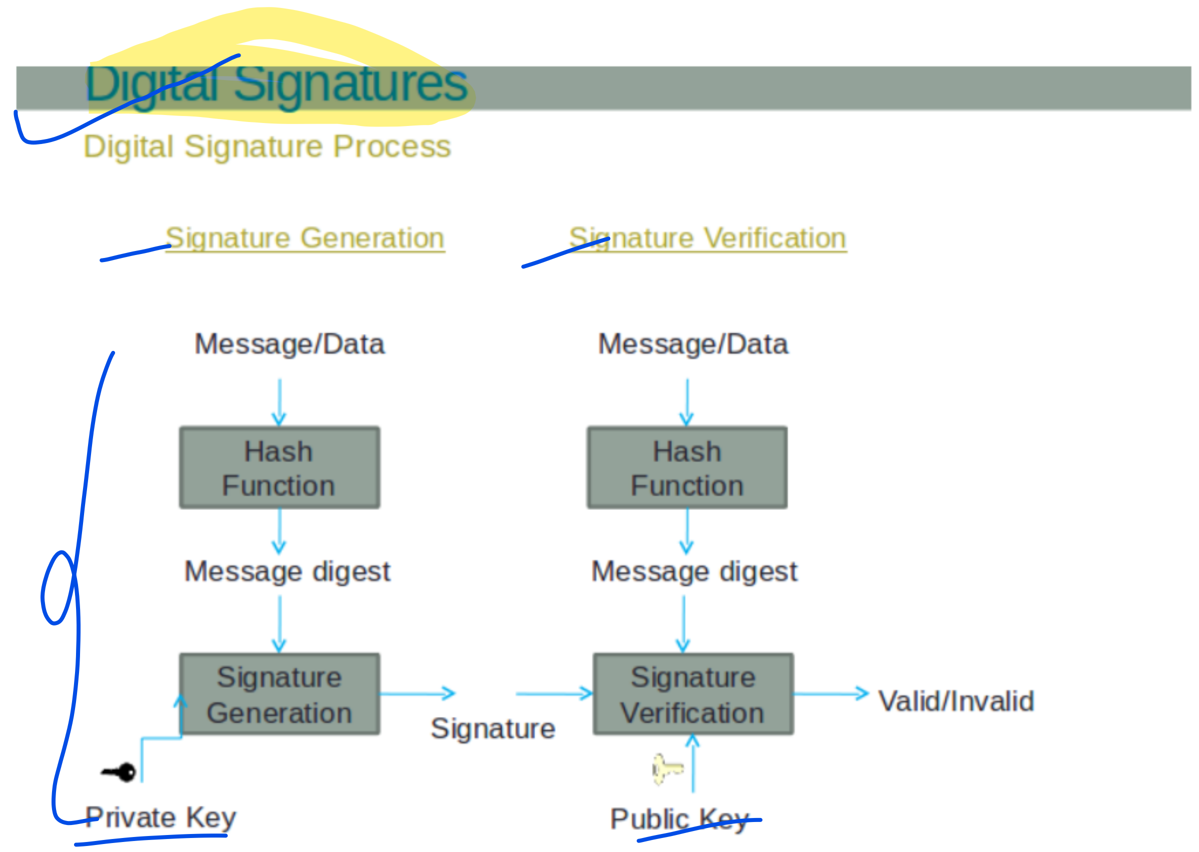
AES usage – Email , file encryption , disk encryption , wireless networking , cloud computing

Modes of operation in AES – ECB , CBC . OFB . CTR

ECB will yeild same result always hence code can be stored in a codebook

RSA generation steps :

1) Generate public and private key
2) Create hash of message
3) Encrypt hash digest with private key
4) Send message and digital signature to recepient
5) Verify digital signature



Digital Signatures

Digital Signature Process

Signature Generation

Signature Verification

The padding scheme used in RSA, in given youtube video , is known as **PKCS (Public Key Cryptography Standards) version 1.5 padding**. This padding scheme is used to enhance the security of RSA encryption by introducing randomness into the plaintext before encryption.

Enhanced Security:

The primary purpose of this padding scheme is to enhance the security of RSA encryption. In basic RSA encryption, encrypting the same message multiple times results in identical ciphertexts, which can leak information about the plaintext.

Keeping different encryption format everytime :

By introducing randomness (r) into the plaintext before encryption, PKCS 1.5 padding prevents deterministic encryption, making it harder for attackers to identify patterns in the ciphertext.

Padding Oracle Attacks:

PKCS 1.5 padding is not entirely secure. One major limitation is vulnerability to padding oracle attacks, such as Bleichenbacher's attack

Lack of Rigorous Security:

PKCS 1.5 padding was designed to add some level of security to RSA, but it does not provide the same level of security as modern padding schemes like RSA-OAEP (Optimal Asymmetric Encryption Padding).

The **whois command** is a powerful tool that can be used to gather information about domain names, IP addresses, and network devices.

attacks that can be performed by whois command -

a) Social engineering attacks - individual target
b) DNS attack
c) IP address spoofing
d) Fraudulent domain registration

The **traceroute command send ICMP packet** to hops and each packet has TTL set to low value , TTL value will be decremented on next hop and if packet does not reach destination then TTL is exceeded

The traceroute command can also be used to measure the **round-trip time (RTT)** for each hop. The RTT is the time it takes for a packet to travel from the source host to the destination host and back again. The RTT can be used to identify potential bottlenecks in the network.

The **dig command is a tool for querying Domain Name System (DNS) servers.** It can be used to lookup the IP address of a domain name, the hostname of an IP address, and other DNS records.

Nikto is an open source web server and web application scanner. Nikto can perform comprehensive tests against web servers for multiple security threats, including over 6700 potentially dangerous files/programs. Nikto can also perform checks for outdated web servers software, and version-specific problems.

nikto vulnerabilities - directory indexing (directory content visible) , outdated software

Due to directory indexing source code is visible and remote control is available

theHarvester is a neat information-gathering tool used by both ethical and non-ethical hackers to scrape up emails, subdomains, hosts, employee names, open ports, and banners from different public sources like popular search engines, PGP key servers, and the Shodan database.

Eg:-

theharvester -d microsoft.com -b pgp, searches for e-mail accounts for the domain microsoft.com in a PGP server

The dmitry (deepmagic information gathering tool) command in Linux is a command-line tool that can be used to gather information about a computer's hardware. It can be used to identify the computer's make and model, the processor type, the amount of memory, the hard drive size, and other information.

The dmitry command is a powerful tool that can be used to troubleshoot hardware problems.

commands -

whois url

whois -h (host)

whois -p (port)

whois -a (search all mirrored database)

whois -d (return reverse delegation object)

nikto -h tsec.edu

theHarvester -d tsec.edu

The **nslookup (name server lookup)** command is used to query DNS (Domain Name System) servers to obtain domain name or IP address information. It is commonly used to troubleshoot DNS-related issues and to gather basic information about DNS records.

When you run the nslookup command, it typically returns information such as the authoritative DNS server for the domain, the IP address corresponding to the domain name, and other related DNS records, such as mail exchangers (MX records) and name servers (NS records). The output might also include details about the DNS server used for the lookup and the query time.

reconnaissance tools - whois , dig ,tracerourte , nslookup , theHarvester

Tcpdump is a command-line packet analyzer that allows you to capture and analyze network traffic in real-time. It's commonly used for troubleshooting network issues, analyzing network behavior, and diagnosing problems related to network communication. tcpdump captures packets as they travel through a network interface and provides detailed information about each packet, including source and destination addresses, protocol information, payload data, and more.

tcpdump commands -

```
tcpdump -i eth0 (record all traffic)
tcpdump host 192.168.0.1 (record traffic to only given ip address)
tcpdump port 80
tcpdump icmp
tcpdump src ip_addr
tcpdump dst ip_addr
tcpdump tcp port port_no
tcpdump -c 10 (capture 10 packet)
tcpdump -i eth0 -w output.pcap (packet capture and store it)
```

Port Scanning - It involves probing a host or network to discover open ports, which act as gateways for network services or applications. These ports are the entry points through which data flows in and out of a system.

Nmap, short for "Network Mapper," is a versatile and widely used open-source tool for network discovery and security auditing. Developed by Gordon Lyon, also known as Fyodor, Nmap has earned a reputation as the go-to tool for port scanning due to its comprehensive feature set and cross-platform compatibility.

States of Port :

Open: An "open" port is one that is actively listening for incoming connections.

Closed: A "closed" port is one that is not actively listening for connections. It means there is no service or application running on that port.

Filtered: A "filtered" port is one that cannot be determined as open or closed with certainty.

Unfiltered: An "unfiltered" port is one that is accessible and can be reached, but its status (open or closed) remains undetermined

Open | Filtered: This state combines characteristics of both open and filtered ports. It suggests that the port is reachable, but the response to a probing request is filtered, possibly by a firewall.

Closed | Filtered: This state also combines characteristics of both closed and filtered ports. It implies that the port is accessible, but the response is filtered, typically indicating that a firewall is blocking probing attempts.

nmap -sT target (TCP scan) - if a port is open connection is established

nmap -sS target (TCP SYN scan) - if port responds with SYN-ACK packet then it is considered open , if RST packet then port is closed

nmap -sF target (FIN scan) - if port is open ignore , else respond with RST packet

nmap -sN target(NULL scan) - similar to FIN scan but can bypass more firewall , if open ignore , if closed RST packet

nmap -sX target(XMAS scan) - similar to null and fin scan

nmap -sA target(Ack scan) - ACK packet sent to port , open respond with RST packet while filtered ports may not respond , hence packet filter firewall can be identified

nmap -sn target_range(ping sweep) - not a scan , but used to identify live host , hence saves time

nmap -sV target(service and version detection) - identify open ports to gain insights about services

nmap -p ports target (port and port range) - specify port or port ranges for scanning

nmap -O target(OS fingerprinting) - attempt to identify the operating system running on the target by analyzing network responses and characteristics.

DOS attack common types - SYN flood , ICMP flood , SMURF

SYN flood - client sends SYN packet to server , then server sends SYN-ACK packet and then client sends ACK packet to server . In this attack handshake is not completed as client sends flood of SYN packet to server and server waits for ACK packet indefinitely hence cannot accept legitimate connections

ICMP flood - client sends ICMP echo packet to server and then server sends response , consume bandwidth and system resource

SMURF - here attacker will spoof IP address and then send ICMP echo packets to server and then server responds with ICMP echo response packet , this causes DOS attack

hping3 -c 15000 -d 120 -S -w 64 -p 80 –flood –rand-source 192.0.0.1

-c 15000 = send 15000 packets

-d 120 = data portion of packet is 120 bytes

-S = sets SYN flag for TCP packet

-w 64 = window size is 64

-p 80 = port 80

iptables is firewall installed by default on Ubuntu distribution

scenario for IP table - input , output , forward actions in iptables - accept , drop ,reject

command -

```
iptables -L ( list all rules)
sudo iptables -A INPUT -p tcp --dport ssh -j ACCEPT
sudo iptables -F (flush iptable)
sudo iptables -A INPUT -p icmp -j DROP (drop icmp packet)
sudo iptables -A INPUT -s 192.168.92.11 -p icmp -j DROP (drop icmp packet
from specific source)
```

BuiltIn table in IP table - Filter Table(Input,Output,Forward) present by default , NAT table (prerouting , postrouting , output) , Mangle Table(Prerouting , Postrouting , Input , Output , Forward) , Raw Table(prerouting , output)

Snort is an open-source, signature-based Network Intrusion Detection System (NIDS) that is capable of performing real-time traffic analysis and packet logging on IP networks. It is widely used for detecting and preventing various types of network intrusions, including probes, attacks, and other types of suspicious traffic.

Modes of operation of snort - Sniffer (packet sniffer , no active IDS) , Packetlogger (capture and log n/w traffic defined by log files) , NIDS , IPS(detect intrusion and take appropriate measures to prevent spread)

Public Key Ring - contain public key of users , whenever anyone wants to send some message to user then his public key will be used and then appropriate private key will be used to decrypt the message , public key ring is stored by exporting file or adding to PGP server

Private Key Ring - contain private keys of user , generally protected by private key or paraphrase . private key is used to decrypt the message and sign the documents

contents of public and private key - user’s name ot email address , user’s fingerprint , key algorithm , key expiration date

```
gpg –full-generate key

gpg –list-keys (list keys in public key ring)

gpg –list-keys niranjan180280@gmail.com (list keys in public keys for specific user )

gpg --export -a Niranjan>senderpublickey (sender public key stored in file)

gpg --export-secret-key -a Niranjan>senderprivatekey (sender private key stored in file)

gpg –fingerprint niranjan180280@gmail.com (sender fingerprint)

gpg –sign-key grey180280@gmail.com (sender sign receiver public key)

gpg --encrypt --sign -r receiver_mail name_of_document_to_be_encrypted

gpg -o outputfile -d document_tobe_encrypted.gpg (decrypt encrypted file)
```

Hashing is a fundamental concept in computer science and cryptography. It involves the transformation of input data (such as a file, password, or message) into a fixed-size value or hash code, typically represented as a sequence of characters or numbers.

Different Hashing Algorithms:

MD5 (Message Digest Algorithm 5): MD5 produces a 128-bit hash value. However, MD5 is considered weak and insecure due to vulnerabilities that allow for collision attacks.

SHA-1 (Secure Hash Algorithm 1): SHA-1 produces a 160-bit hash value. Like MD5, SHA-1 is also considered weak and has been deprecated in favor of more secure algorithms.

SHA-256, SHA-384, SHA-512: These are part of the SHA-2 family and produce hash values of different lengths (256, 384, and 512 bits, respectively). They are widely used and considered secure for many cryptographic applications.

SHA-3: The latest member of the Secure Hash Algorithm family, SHA-3 produces hash values of various lengths and is designed to be highly secure and resistant to known attacks.

bcrypt: A key derivation function commonly used for securely hashing passwords. It incorporates a work factor that slows down hashing and makes brute-force attacks more difficult.

Argon2: A state-of-the-art key derivation function that won the Password Hashing Competition. It's designed to be memory-hard and resistant to various types of attacks.

HMAC (Hash-based Message Authentication Code): Not a standalone hash algorithm, but a construction that uses a hash function in combination with a secret key to provide message integrity and authenticity.

BLAKE2: A high-speed cryptographic hash function that is an improvement over SHA-2 and SHA-3 in terms of performance.

Options in hashdeep -

-c (compute hash with algorithm specified , computation mode)

-k (load file of known hashes , required during auditing)

-a (audit mode, each input file is compared with known files and audit is passed if match is found else failed)

-m (positive matching, only matched files are printed)

-x (negative matching, only non matched files are printed)