Date

Lecture 1-4 :-

Physical Security, Personal Security, Operations Security → Well-Secured Organization

Communications Security, Network Security

Security : free from danger

Information Security : protection of info & its critical elements, including systems & hardware that use, store, and transmit that info.

C.I.A triangle : Confidentiality, integrity, availability

1

Critical Characteristics of Info :

1.) Timeliness : no value if too late
2.) Availability : no interference/obstruction, required format
3.) Accuracy : free from mistakes
4.) Authenticity : state of being genuine
5.) Confidentiality : No exposure to unauthorized individuals/system
6.) Integrity : uncorrupted
7.) Possession : ownership (breach of confidentiality results in breach of possession)

Information Security is entire set of software, hardware, data, people, procedures, and networks necessary to use info as a resource in the organization.

Software
- difficult to secure
- easy target
- most attacks are on info

Hardware
- physical security policies
- secure physical location

Data
- most valuable asset
- main target of attacks

People
- weakest link
- social eng
- must be well-trained & informed

Procedures
- threat to integrity of data

Networks

Date

(2)

=> Risk Estimation :-

1.) Assets : Objects, data, people
2.) Vulnerability : Weakness of Asset
3.) Threat : loss of security due to vulnerability
4.) Attack : threat occurence

Risk Estim is the process of identifying vulnerabilities & threats & their impact & probability of occuring an attack.

=> Data Protection :-

- most valuable asset is data
- without data, an org loses its record of transactions & its ability to deliver value to its customers
- effective information security program is essential to protect the integrity & value of organization's data
- organizations should have secure infrastructure services based on size & scope of org

=> Threats :-

- threat is an object / person / entity that represents constant danger to asset
- management should be well-informed about threats

=> Threat Modelling : Theoretical use cases considered to identify potential threats.

(Microsoft Stride)

S	T	R	I	D	E
spoofing of identity	tempering w data	repudiation	info disclosure	denial of service	elevation of privelege

Date

⇒ Attacks: deliberate act that exploits vulnerability
(accomplished by a threat-agent to damage or steal an org's info or asset

Exploit: technique to compromise a system
→ attack is the use of an exploit to achieve the compromise of a controlled system

~ Classes of Attacks ~

① Phishing :-

- attempt to steal sensitive info (usernames, passwords, credit card numbers, bank acc info). Pretends to be a reputable source with enticing request.
- Occurs via email or instant message
- Send fraud emails/messages that appear to be from a trusted source such as bank or govt agency → redirect to a fake login page where user is prompted to enter login credentials.

→ Spear Phishing : targeted attack that uses personalized messaging, esp emails.

→ Vishing : Voice phishing, attackers spoof the calling phone num to appear as if its coming from a bank/institute.

→ Smishing : SMS phishing

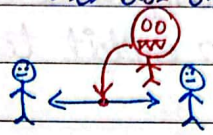
② Backdoor Attack :-

- sidestepping normal authentication procedures to gain unauthorized access to a system. involves exploiting system weaknesses or installing malicious software that creates an entry point for the attacker.

Date

③ Password Creck: process of guessing passwords protecting: ca computer system

Brute force	Dictioncary
try every possible combination	uses list of commonly used passwords

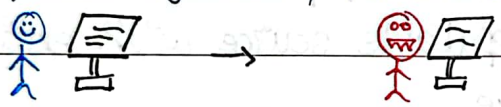


④ Packet-Sniffing / Eavesdropping

passwords/sensitive dater are read by unauthorized 3rd parties

⑤ Ip Spoofing / Mesquerading

creation of ip packets with a false source ip address to impersonate another computer system. // someone takes the plece of the legitimate host



⑥ Connection Hijacking / Data Spoofing / Alteration

dater is modified during the transmission

⑦ Denial-of-Service (DoS)

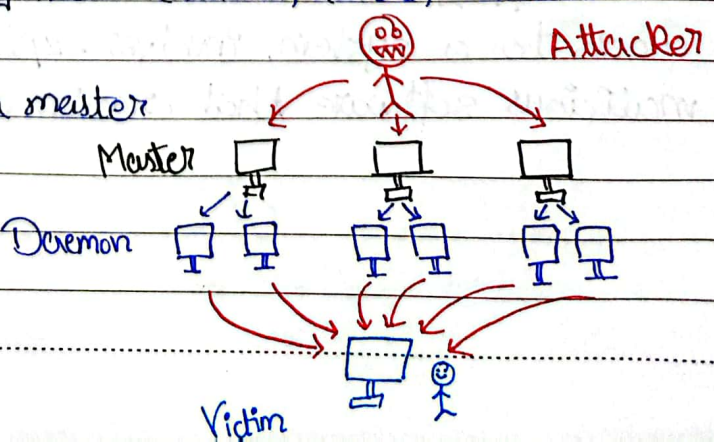
disrupt or shut down the normal functioning of a targeted server, service or network by overwhelming it with a flood of illegitimate requests that trigger a crash. // flood target machine with requests until normal traffic is unable to be processed e.g ping bombing

⑧ Distributed Denial of Service (DDoS):

① Software for DoS installed on many nodes (daemon, zombie, malbot) to create a Botnet.

② Daemons remotely controlled by a master

③ Effect of DoS attack x Daemons



Date

=> Security Principles <=

1.) Least Privelege :- limit accessible data, resources, applications to only that which a user/entity requires to execute their specific task.
→ Without this, org create over-priveleged users/entities that increase the potential for breaches & misuse of critical systems & data.
→ damage caused by compromised user/app is reduced.

2.) Separation of Privelege :- division of system priveleges or access rights to ensure that no single entity possesses all the necessary permissions to compromise the security of a system or access critical resources
→ Multiple conditions should be required to achieve access to restricted resources

3.) Fail Safe Defaults :- access to an object or resource should be denied by default until explicitly granted. vital in minimizing security vulnerabilities & preventing unauthorized access to sensitive info.
e.g firewall rules, access control lists

4.) Complete Mediation :- every access to every object should be authorized. Access should be checked, e.g not only when a file is opened, but also on each subsequent read/write to that file. Do double checking, whenever user wants to read file, check access.

Keep it simple

5.) Economy of Mechanism :- security mechanisms should be as simple as possible. If a design & implementation are simple, fewer possibilities exist for errors. The checking & testing process is less complex, cuz fewer components & cases need to be tested. fewer errors, less assumptions

Date

6.) Least common mechanism :- Limits sharing, mechanisms used to access resources should not be shared. disallows the sharing of mechanisms that are common to more than one user or process if the users or processes are at different levels of privelege. Separate channel for users, separation of network resources.

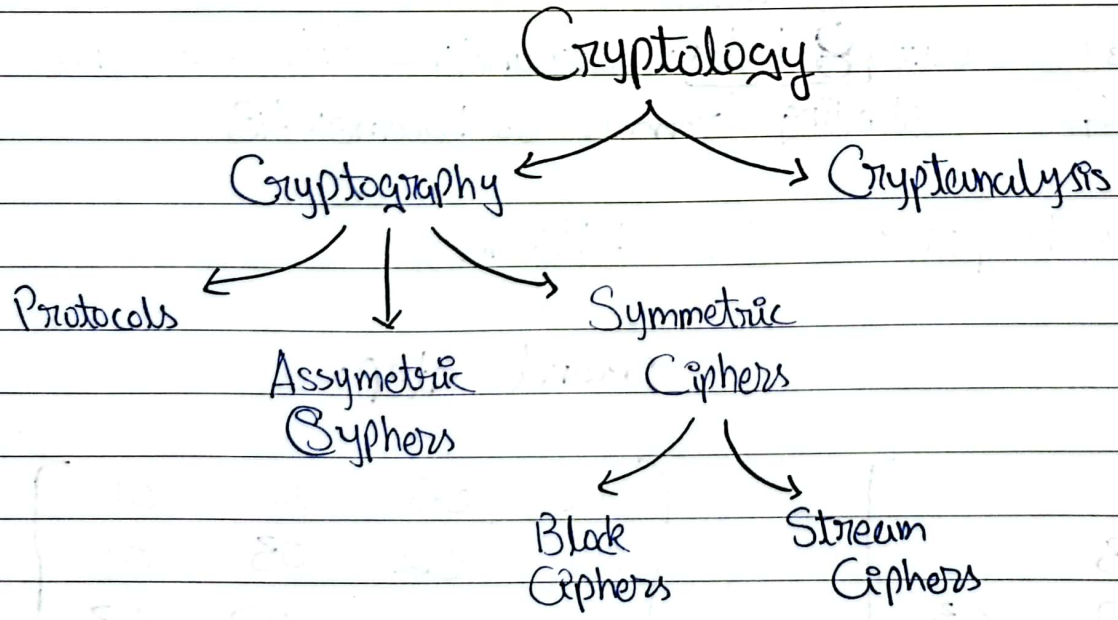
7.) Psychological Acceptability :- security mechanisms should not make the resource more difficult to access than if the security mechanisms were not present. Configuring & executing a program should be as easy & as intuitive as possible & any output should be clear, direct & useful. UI → well designed & intuitive

8.) Open Design :- your system security should not rely on the secrecy of your implementation. Well-designed cryptography implementations are published publicly.

Date 6 Sep, 24

Lecture 3 :-

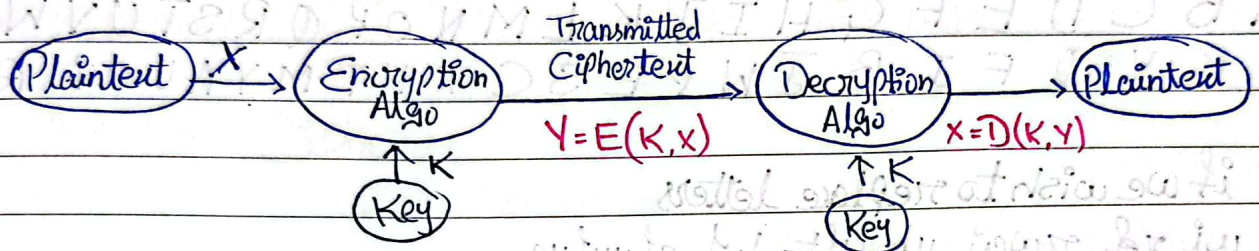
Plaintext : original msg
Ciphertext : coded msg
Encryption Algo: algo for transforming : plain text → cipher text
Key: info used in cypher, known only to sender/receiver
Encipher: convert plain text → cipher text
Decryption Algo: algo for ciphertext → plaintext
Decipher: convert ciphertext → plaintext
Cryptography: study of encryption principles/methods
Cryptanalysis: study of principles/methods of deciphering ciphertext without knowing key
Cryptology: field of both cryptography & cryptanalysis



Date

Symmetric Cryptography :-

→ sender/recipient share common key
→ all classical encryption algo are private-key



2 requirements :-
1.) strong encryption algo
2.) secret key known only to sender/r

1) Classical Substitution :-

1) Caesar Cipher :-

→ earliest known substitution cipher
→ first attested use in military affairs

replace each letter by 3rd letter

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

m e e t m e a f t e r t h e t o g a p a r t y
p h h w p h d i w h u w k h w r j d s d u w b

→ only 25 keys possible
→ brute force search is easy

Date

2.) Monoalphabetic Cipher :-

→ each plaintext letter maps to ei diff random ciphertext letter
→ Key is 26 letters long

Q Z N
X Y Z

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

Plaintext : if we wish to replace letters
wi rq rwcj uh yftsdvt sfuufyq

→ Keys possible : $26! = 4 \times 10^{26}$ human lang are redundant
→ problem : language characteristics

eng letter frequencies :-
1.) e 2.) t 3.) a 4.) O 5.) i 6.) n 7.) S 8.) h

→ monoalphabetic substitution ciphers dont change relative letter frequencies
→ calculate letter freq for ciphertext
→ compare counts/plots against known values
→ for monoalpha must identify each letter

3.) Vigenère Cipher :-

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	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Plaintext + Key	d	e	c	e	p	t	i	v	e	d	e	c	e	p	t	i	v	e	d	e	c	e	p	t	i	v	e
	3	4	2	4	15	19	8	21	4	3	4	2	4	15	19	8	21	4	3	4	2	4	15	19	8	21	4
	22	4	0	17	4	3	8	18	2	14	21	4	17	4	3	18	0	21	4	24	14	20	17	18	4	11	5
	w	e	a	r	e	d	i	s	c	o	v	e	r	e	d	s	a	v	e	y	o	u	r	s	e	l	f
Cipher	z	i	c	v	t	w	q	n	g	r	z	q	v	t	w	a	v	z	h	c	a	y	q	l	m	q	i
	25	8	2	21	19	22	16	39	6	17	25	6	21	19	22	26	21	25	7	28	16	24	32	37	12	32	9

-26=13

Date

letter frequencies are obscured but not totally lost

4.) Kasiki Method :-

repetitions in ciphertext give clues to period, find same plaintext an exact period apart which results in same ciphertext then attack each monoalphabetic cipher individually using same techniques as b4

5.) AutoKey Cipher :-

- ideally want a key as long as message
- Vigenere proposed the autokey cipher with keyword is prefixed to message as key knowing keyword can recover the first few letters
- still have frequency characteristics

Key: deceptive wearediscoveredsav
Plaintext: wearediscoveredsaveyourself

the key & the plaintext may share the same frequency dist of letters, a statistical tech can be applied for cryptanalys

6.) One-time Pad :-

- if a truly random key as long as the message is used, the cipher will be secur called a one time pad.
- unbreakable since ciphertext bears no stastical relationship to the plaintext
- key can be used only once

NOT Practical :-

1.) large number random key formation
2.) distribution & protection among parties

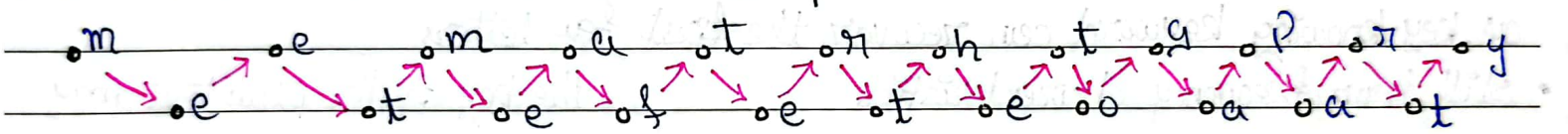
Date

Classical Transposition :-

- hide the message by rearranging the letter order without altering the actual letters used
recognize these since have the same frequency distribution as the original text

1.) Rail-Fence Cipher :-

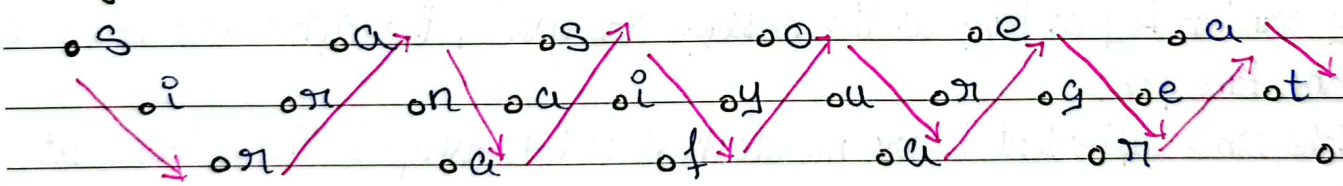
plaintext: meet me after the toga party 23 letters so 23 dots



ciphertext: mematrhtgpryetefeteoeat

ciphertext: sasoecairnaiyurgetrcafar 22 dots

Key: 3



plaintext: sir rena esif you ere greet

2.) Row Transposition Ciphers

write letters of message out in rows over a specified number of column
then reorder the columns according to some key

	4	3	1	2	5	6	7
Plaintext:	a	t	t	a	c	k	p
	o	s	t	p	o	n	e
	d	u	n	t	i	l	t
	w	o	a	m	x	y	z

Key: 4312567

thnaptm tsuo aodw
coix knly petz

Date

- recognizable as same letter frequencies as original text
- made secure by performing more than one stage of transposition

Bit-Oriented Ciphers :-

- numbers, graphics, audio & video data

1.) Stream Ciphers :-

- process a bit/byte at a time when encrypting/decrypting : Vernam Cipher.
- if cryptographic keystream is random, cipher is unbreakable
- Bit-stream generator is a key controlled algo & must produce a bit stream that is cryptographically strong

Data :	0	0	1	0	1	1	0	1	1	1
Key :	1	0	0	1	1	0	0	0	0	1
Cipher :	1	0	1	1	0	1	0	1	1	0

(XOR)

Cipher :	1	0	1	1	0	1	0	1	1	0
Key :	1	0	0	1	1	0	0	0	0	1
Data :	0	0	1	0	1	1	0	1	1	1

(XOR)

2.) Block Ciphers :-

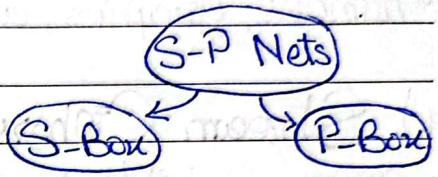
- process message in blocks of bits, like a substitution on v big characters 64-bits / 128
- many current ciphers are block ciphers.

Date

Lecture 5 :-

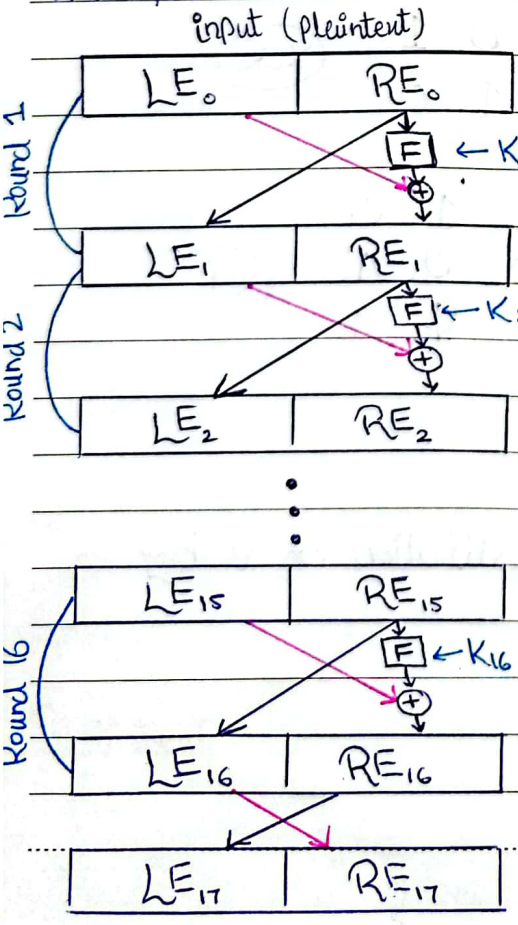
1) Claude Shannon & Substitution-Permutation Ciphers :-

- Claude Shannon introduced idea of SP networks in 1949 paper
- form basis of modern block ciphers
- provide confusion & diffusion of msg & key
  - confusion ← substitution
  - diffusion → permutation

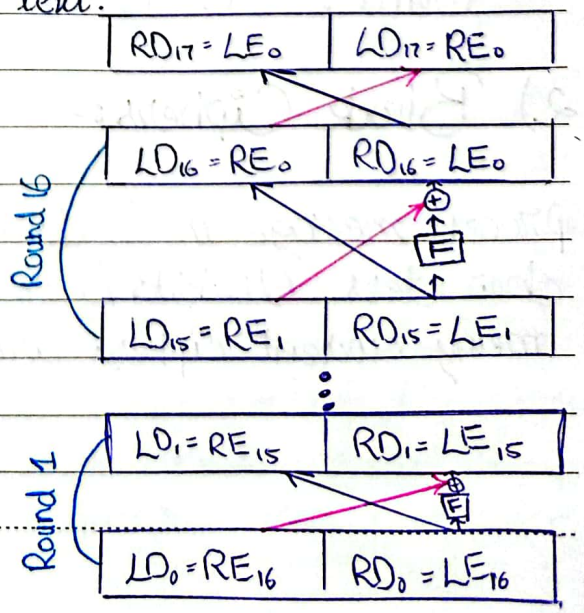


2.) Feistel Cipher :-

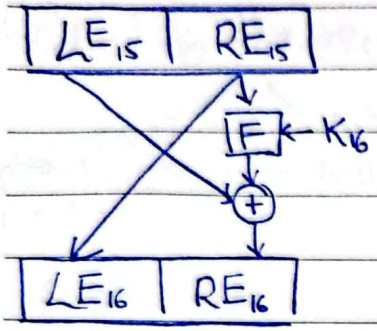
- utilize the concept of a product cipher
- alternates substitutions & permutations
- practical application of proposal by Claude-Shannon
- key length of k bits, block length of n bits, allow a total of 2^k transformations.



input divided into 2 parts e.g if plaintext is 64 bits then each side is 32 bits.
Key is also called round key cuz each round has diff key. 16 rounds in total.
After round 16, swap will take place which will give us the cipher text.



Date

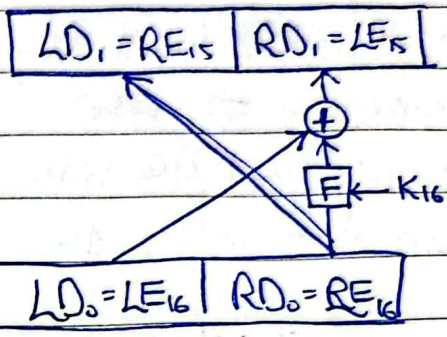


$LE_{16} = RE_{15}$

$RE_{16} = LE_{15} \oplus F(RE_{15}, K_{16})$

$RD_1 = LD_0 \oplus F(RD_0, K_{16})$

$\rightarrow RE_{16} \oplus F(RE_{15}, K_{16})$



Round 16

$$RD_1 = \left[LE_{15} \oplus F(RE_{15}, K_{16})\right] \oplus F(RE_{15}, K_{16})$$

$$= LE_{15} \oplus \left[F(RE_{15}, K_{16}) \oplus F(RE_{15}, K_{16})\right]$$

$$= LE_{15} \oplus 0$$

$$RD_1 = LE_{15}$$

features:-

- → block size
- → key size
- → num of rounds
- → subkey generation algo
- → round function
- → fast encryption/decryption algo
- → ease of analysis

Date

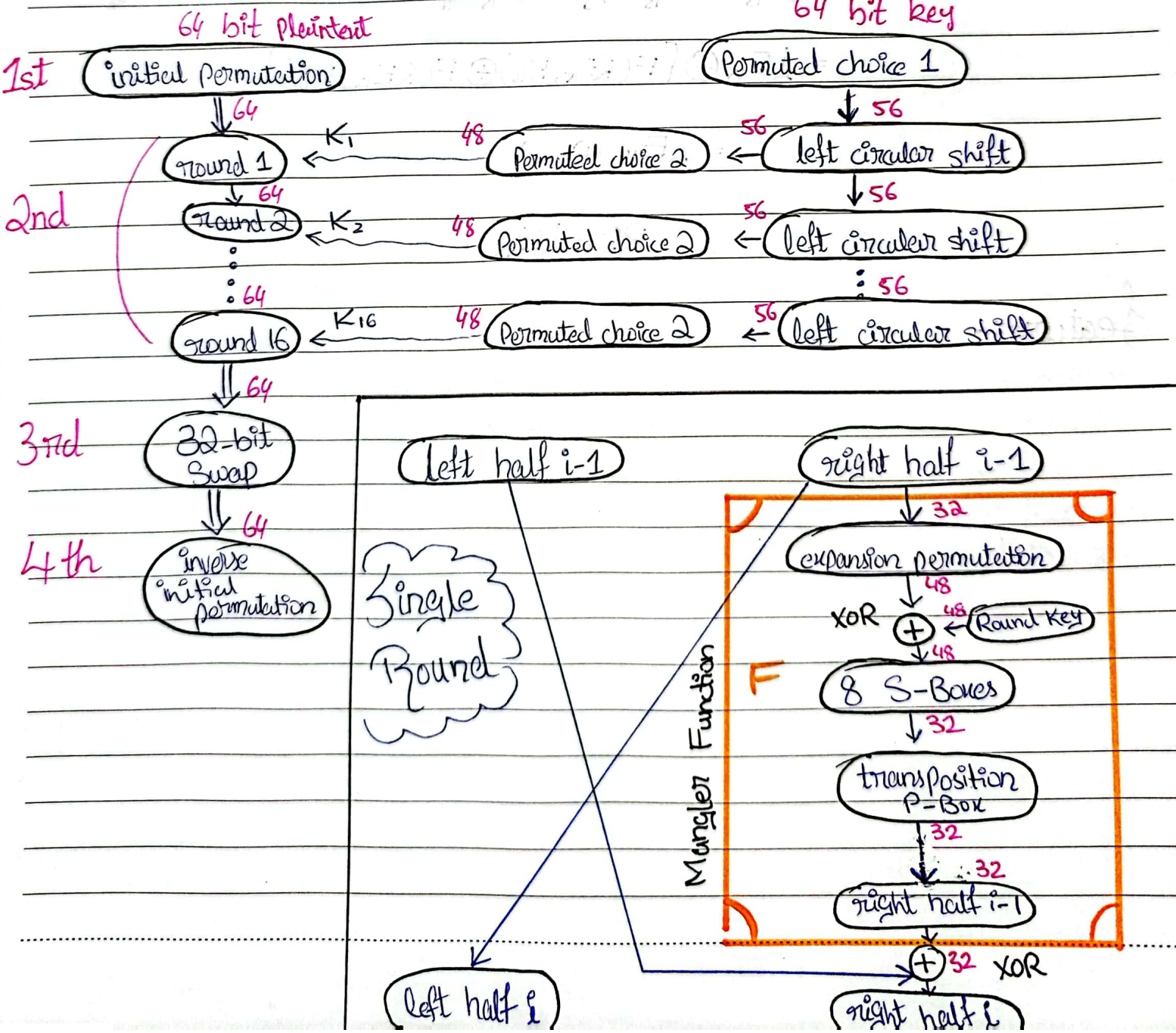
3.) Data Encryption Standard: DES

- encrypts 64-bit data using 64-bit key

exact structure as feistel
- initial permutation
- final permutation of last round

input | output | main key = 64 bits
subkey : 56 bits
round key : 48 bits
num of rounds : 16

Each round is given 64 bits into it & it outputs 64 bits



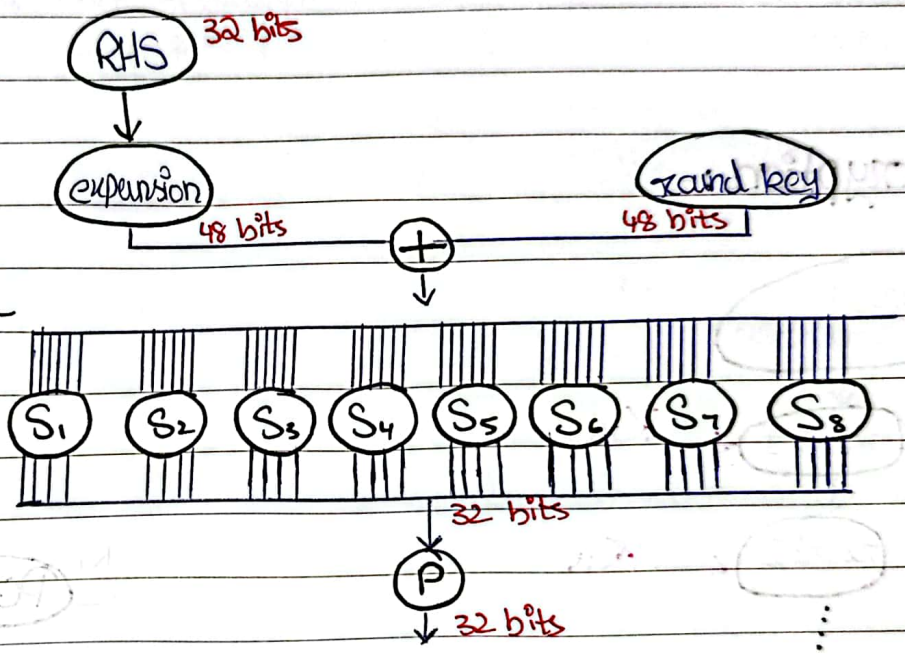
Date

Roles of S-Boxes :-

- 8 S-Boxes, each has 6-bit input, 4 bits out
- outer 2 bits (1,6) used to select row
- inner 4 bits (2-5) used to select column

8 4-bit groups : 32 bit output

input 011001
row 01 : 1
column 1100 : 12



Mangler Function :-

1.) expansion
2.) XOR with key
3.) S-Box
4.) P-Box

1.) Expansion :-

32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1
8		32		8	

= 48 bits

4.) P-Box :-

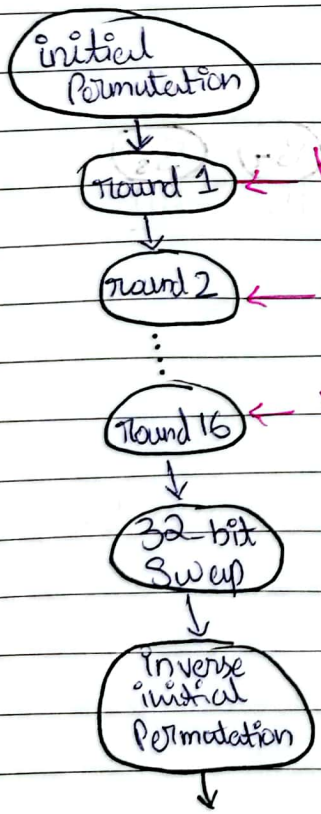
A table is given ; it just changes the positi of the bits. Used for diffusion

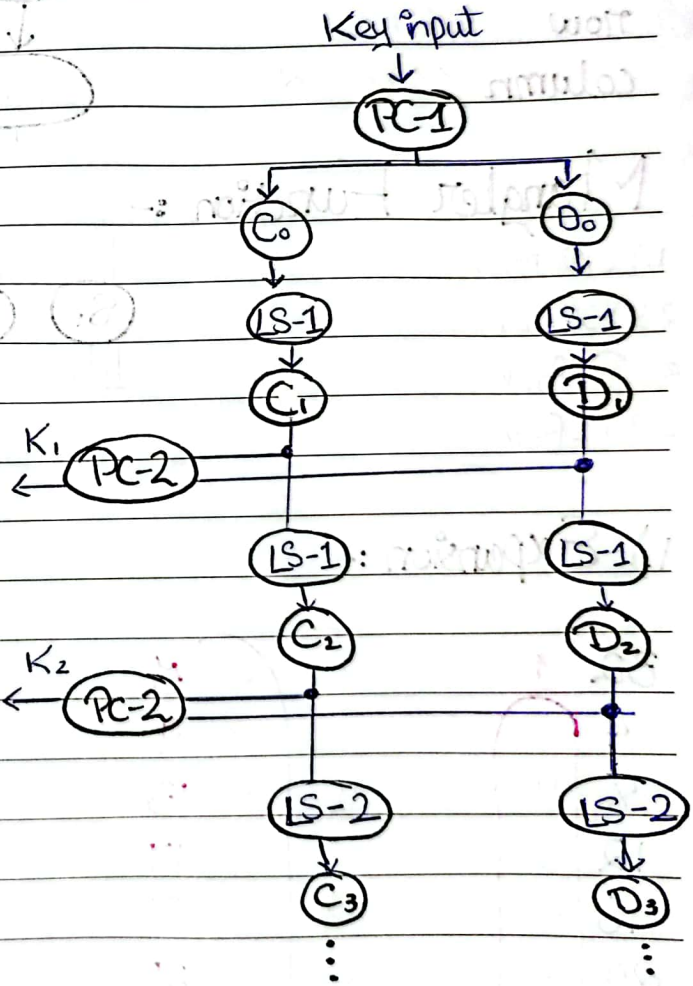
Date

Key Scheduling :-

- 64 bit input is given to permuted choice 1 & it gives 56 bits
  ↳ the bits dropped are : 8, 16, 24, 32, 40, 48, 56, 64
- The 56 bit key is called the Effective Key.
- Left Shift : 1 shift for rounds 1, 2, 9, 16
  2 shift for all other rounds
- Permuted Choice 2 gets 56 bit input, 8 bits are dropped & 48 bits are permuted

Decryption :-





just order of the round keys is changed.

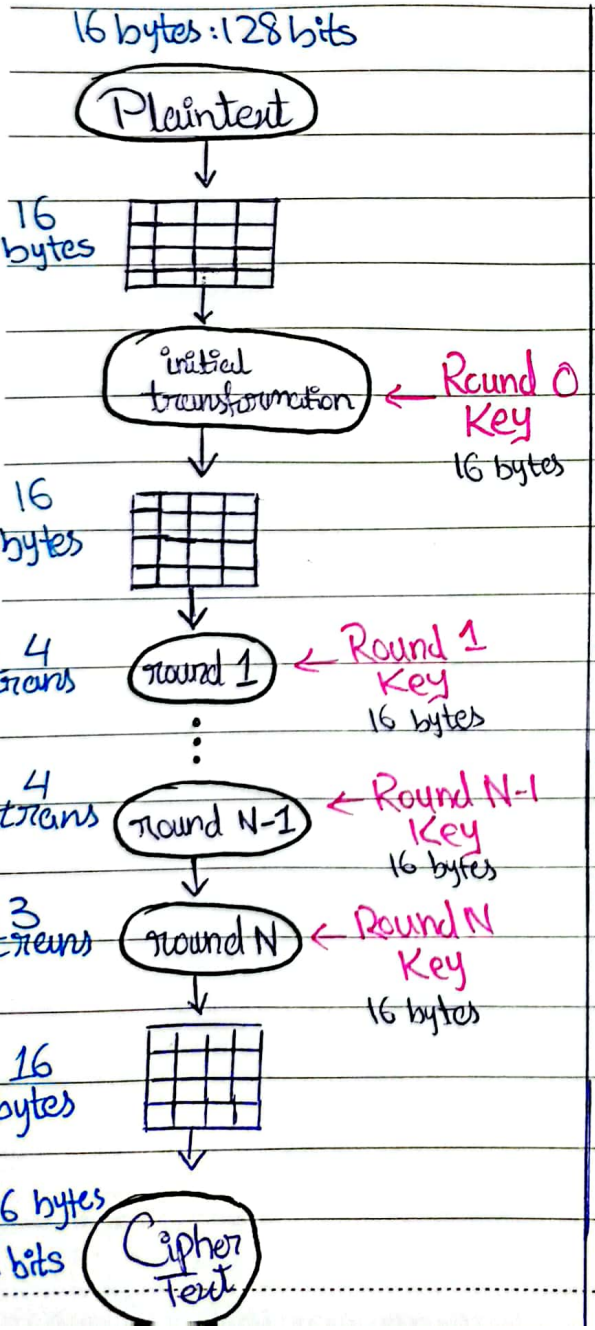
Date 9 Sep '24

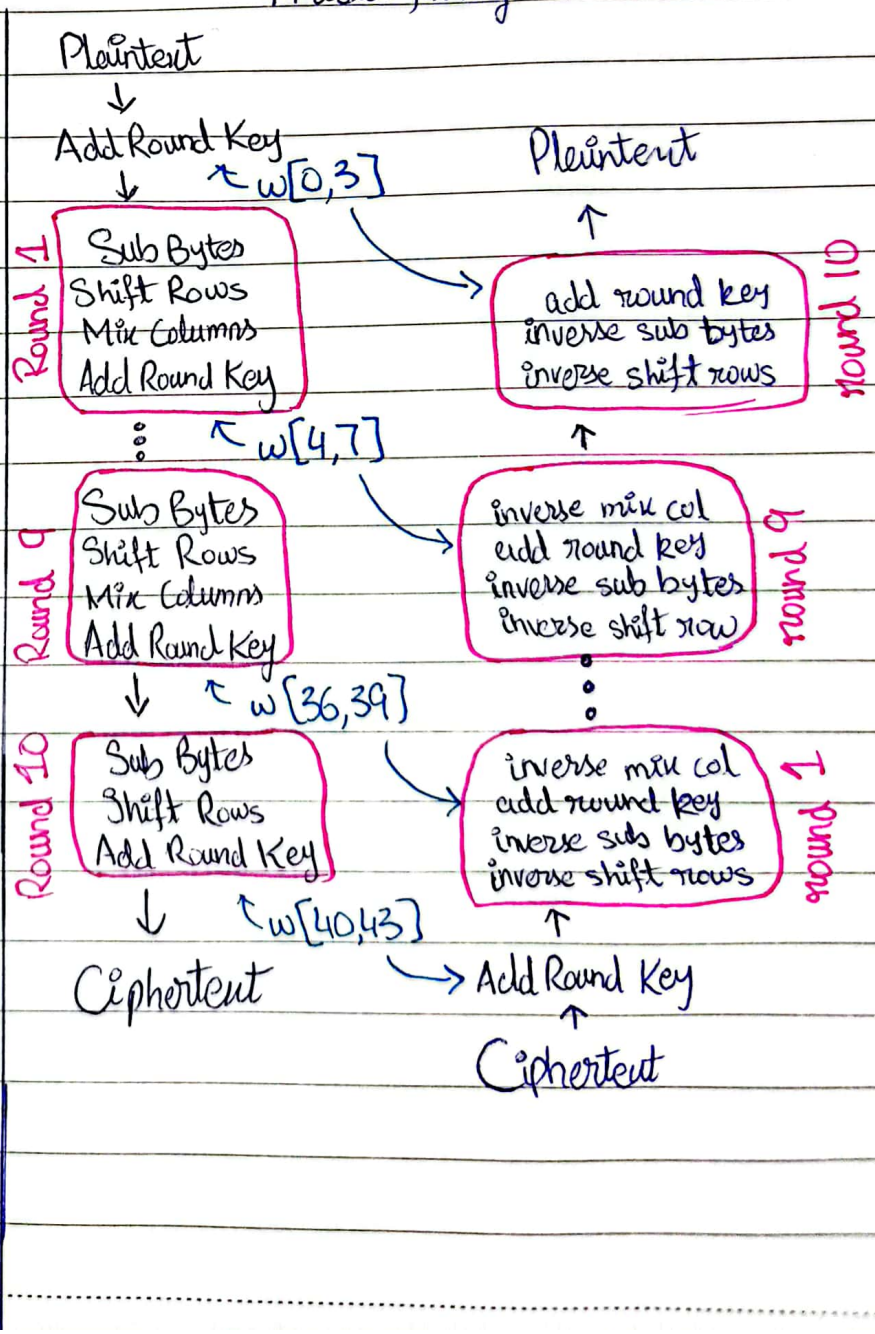
Tuesday
8:51

Lecture 6 :-

Advanced Encryption Standard (AES) :-

	AES-128	AES-192	AES-256
Key Size	128	192	256
Plaintext Size	128	128	128
Num of Rounds	10	12	14
Round Key Size	128	128	128



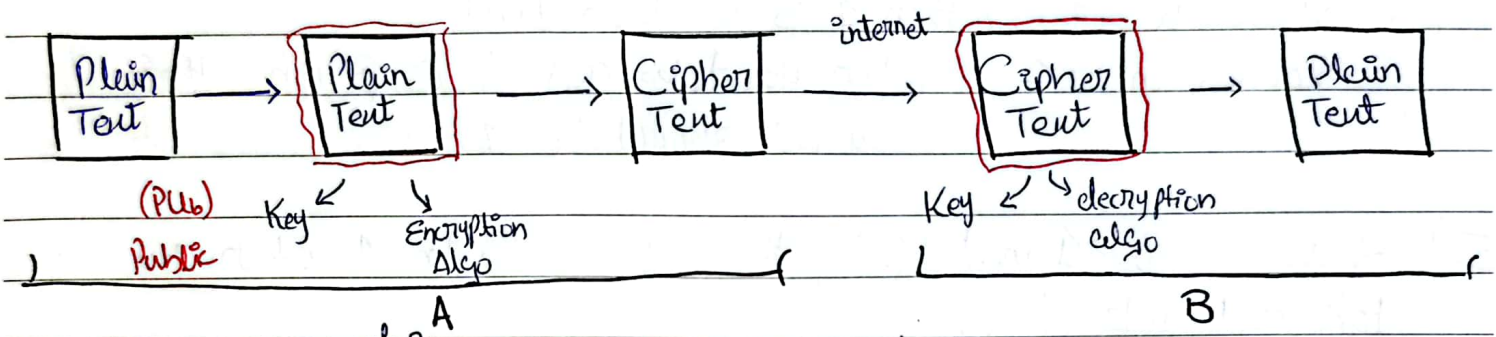


Date

Lecture 7 : RSA

Assymetric Encryption :-

- public key / two keys



Use the public key of B at source to encrypt it & use the private key at destination to decrypt it

if you use private key to encrypt then it will create a signature

⇒ RSA :-

① Take 2 prime numbers : p & q ($p \neq q$)

② Calculate n, $n = p \times q$

③ find ϕ

e.g $\phi(5) = ?$ so we need to choose the gcd

gcd(1,5) = 1
gcd(2,5) = 1
gcd(3,5) = 1
gcd(4,5) = 1
$\phi(5) = 4$
count number of 1s

$\phi(8) = ?$
gcd(1,8) = 1
gcd(2,8) = 2
gcd(3,8) = 1
gcd(4,8) = 4
gcd(5,8) = 1
gcd(6,8) = 2
gcd(7,8) = 1

$\phi(8) = 4$

Date

if n is a prime num $\phi(n) = n-1$

$\phi(5) = 4$

$\phi(7) = 6$

if n is in the form of $p \times q$

$\phi(n) = \phi(p \times q)$

$= \phi(p) \times \phi(q)$

$= (p-1) \times (q-1)$

4.) Select encryption key e where:

e should be greater than 1 & less than $\phi(n)$

$\gcd(e, \phi(n)) = 1$ when you take gcd of e & $\phi(n)$ then answer should be 1

5.) Solve $e.d = 1 \bmod \phi(n)$, the ans should be 1 when you take mod, take d value

6.) Encryption : $C = M^e \bmod n$

7.) Decryption : $M = C^d \bmod n$

Example :-

1.) $p = 3, q = 5$

2.) $n = p \times q = 15$

3.) $\phi(n) = (3-1) \times (5-1) = 8$

4.) $d \Rightarrow e.d = 1 \bmod \phi(n)$

$3d = 1 \bmod 8$

$3 \times 3 = 1 \bmod 8$

$d = 3$

$\therefore d = 3$

$9 \% 8 = 1$

5.) $PU = \{e, n\} = \{3, 15\}$

$PR = \{d, n\} = \{3, 15\}$

Encryption:

$C = 2^3 \bmod 15$

$= 8 \bmod 15$

$C = 8$

Decryption:

$M = 8^3 \bmod 15$

$= 512 \bmod 15$

$M = 2$

$M = 2$

Date

Example :-

1.) $p = 17, q = 11$

2.) $n = 17 \times 11 = 187$

3.) $\phi(n) = (17-1) \times (11-1) = 16 \times 10 = 160$

4) $e = 7$

5) $d = ?$ formula: $d = \frac{(\phi(n) \times i) + 1}{e} = \frac{(160 \times 1) + 1}{7} = \frac{161}{7} = 23$

the answer should not be in decimals, take whole number

5) $7.23 = 1 \bmod 160$

$d = 23$

6.) $PU = \{e, n\} = \{7, 187\}$

$PR = \{d, n\} = \{23, 187\}$

$M = 88$ (take by urself)

decimal:

$(88-88) \div (187 \times 187)$

Encryption :

$C = 88^7 \bmod 187$

$C = [(88^4 \bmod 187) \times (88^2 \bmod 187) \times (88 \bmod 187)] \bmod 187$

77×77 ↓ 132 | ↓ 88×88 ↓ 77 | ↓ 88

$C = (132 \times 77 \times 88) \bmod 187 = 11$

Decryption : $M = 11^{23} \bmod 187$ (make groups like 1, 2, 4, 8, 16)

Date

Example :-

① $p = 47, q = 59$

② $n = p \times q = 2773$

③ $\phi(n) = (46) \times (58) = 2668$

④ $e = 3$

⑤

$$d = \frac{(\phi(n) * i) + 1}{e} \quad (i = 1) = \frac{2668 + 1}{3} = \frac{2669}{3} = 889.6$$

$$d = \frac{(2668 \times 2) + 1}{3} = \frac{5336 + 1}{3} = 1779$$

$d = 1779$

6.) $PU = \{e, n\} = \{3, 2773\}$

$PR = \{d, n\} = \{1779, 2773\}$

Date

Activity 2 :-

Q.1 RSA algo is used to encrypt info 3 public key to decrypt msg is {7, 187}. Retrieve original msgs.

$C_1 = 16$, $C_2 = 24$

$PU = \{e, n\} = \{7, 187\}$

$e = 7$, $n = 187$

$n = p \times q$

$187 = 17 \times 11$

so

$p = 17$, $q = 11$

$\phi(n) = (17-1) \times (11-1)$

$= 16 \times 10 = 160$

$$d = \frac{(\phi(n) \times i) + 1}{e}$$

$$d = \frac{(160 \times 1) + 1}{7} = 23$$

so $d = 23$

$PR = \{d, n\} = \{23, 187\}$

$M_1 = C_1^d \bmod n = 16^{23} \bmod 187$

$= [(16^8 \bmod 187) \times (16^8 \bmod 187) \times (16^4 \bmod 187) \times (16^2 \bmod 187) \times (16 \bmod 187)] \bmod 187$

$=$

$= 103$

$16^8 \bmod 187$: $86 \times 86 = 103$

$16^4 \bmod 187$: $69 \times 69 = 86$

$16^2 \bmod 187$: $16 \times 16 = 69$

$16 \bmod 187$: 16

$= (103 \times 103 \times 86 \times 69 \times 16) \bmod 187$

$= 10072608896 \bmod 187 = 169$

$M_2 = C_2^d \bmod n = 24^{23} \bmod 187 = 63$

Q.2 $p=7, q=11, e=7$

$n = p \times q = 77$

$\phi(n) = (p-1) \times (q-1) = 60$

$d = \frac{(60 \times 5)+1}{7} = \frac{301}{7} = 43$

$PU = \{e, n\} = \{7, 77\}$

Assume $M = 2$

$C = M^e \bmod n = 2^7 \bmod 77 = 51$

$M = C^d \bmod n = 51^{43} \bmod 77$

Date

$[(51^{16} \bmod 77) \times (51^{8} \bmod 77) \times (51^{5} \bmod 77) \times (51^{4} \bmod 77) \times (51^{4} \bmod 77) \times (51^{2} \bmod 77) \times (51 \bmod 77)] \bmod 77$

$\downarrow \quad \downarrow \quad \downarrow \quad \downarrow \quad \downarrow \quad \downarrow \quad \downarrow$

$37 \quad 53 \quad 53 \quad 58 \quad 58 \quad 60 \quad 51$

$= (37 \times 37 \times 53 \times 60 \times 51) = 22202420 \bmod 77 = 2$

Q.3 $p = 61, q = 53, m = 10$; use RSA

$n = p \times q = 61 \times 53 = 3233$

$\phi(n) = 60 \times 52 = 3120$

$e = 7$

$d = \frac{(\phi(n) \times i) + 1}{e} = \frac{(3120 \times 4) + 1}{7} = 1783$

$PU = \{e, n\} = \{7, 3233\}$

$C = M^{e} \bmod n = 10^{7} \bmod 3233 =$

$[(10^{4} \bmod 3233) \times (10^{2} \bmod 3233) \times (10 \bmod 3233)] \bmod 3233$

$301 \qquad 100 \qquad 10$

$= (301000) \bmod 3233 = 331$

$C = 331$

$M = C^{d} \bmod n = 331^{1783} \bmod 3233 = 10$

b.) $p = 11, q = 13, e = 7, m = 9$; use RSA

$n = p \times q = 143$

$\phi(n) = 120$

$d = \frac{(120 \times 6) + 1}{7} = 103$

$C = M^{e} \bmod n = 9^{7} \bmod 143 = 48$

$M = C^{d} \bmod 143 = 48^{103} \bmod 143 = 9$

Date

Lecture 8 :-

Diffie-Hellman: Key Exchange :-

not for encryption/decryption

Alice	Bob
1.) suppose prime num q	1.) suppose q
2.) suppose α	2.) suppose α
i) $\alpha < q$	
ii) α is a primitive root of q	$\alpha \bmod q$, $\alpha^2 \bmod q$, $\alpha^3 \bmod q$ => $\{1, 2, 3, \ldots q-1\}$ ⋮ $\alpha^{q-1} \bmod q$
3.) Generate private key X_A	3.) Generate private key X_B
4.) Generate public key $Y_A = \alpha^{X_A} \bmod q$	4.) Generate public key $Y_B = \alpha^{X_B} \bmod q$
	share
5.) Generate Secret Key $K = Y_B^{X_A} \bmod q$	5.) Generate Secret Key $K = Y_A^{X_B} \bmod q$
Should be equal	

Date

Mathematically :-

X_A → Alice Secret Key

$$K = Y_B \bmod q$$
$$= (\alpha^{X_B} \bmod q)^{X_A} \bmod q$$
$$= (\alpha^{X_B})^{X_A} \bmod q \quad > (==)$$

$$K = \alpha^{X_B X_A} \bmod q$$
$$= (\alpha^{X_A})^{X_B} \bmod q$$
$$= (\alpha^{X_A} \bmod q)^{X_B} \bmod q \quad > (==)$$

$$K = (Y_A)^{X_B} \bmod q$$

↳ Bob Secret Key

example: $(2^3 \bmod 3)^2 \bmod 3 == (2^3)^2 \bmod 3$

$(8 \bmod 3)^2 \bmod 3 == 8^2 \bmod 3$

$(2)^2 \bmod 3 == 64 \bmod 3$

$4 \bmod 3 == 1$

$1 == 1$

$2^1 \bmod 11$ $2^3 \bmod 11$ ...

	1	2	3	4	5	6	7	8	9	10
1	1	1	1	1	1	1	1	1	1	1
2	2	4	8	5	10	9	7	3	6	1
3										
4										
5										
6										
7										
8										
9										
10										

Choose a number that has no repetitions. eg if 2 had any repetition we would have taken 3 and so on....

Example :-

$q = 11$, $\alpha = 2$

Randomly generate :-

$X_A = 2$ $X_B = 3$

Public Key :-

$Y_A = 2^2 \bmod 11 = 4 \bmod 11$

$Y_A = 4$ ↓↑ shared

$Y_B = 2^3 \bmod 11 = 8 \bmod 11$

$Y_B = 8$

$K = 8^2 \bmod 11 = 64 \bmod 11$

$K = 9$

Alice Secret Key

$K = 4^3 \bmod 11 = 64 \bmod 11$

$K = 9$

Bob Secret Key

Date

Example :-

$q = 353, \alpha = 3$

$X_A = 97, \quad X_B = 233$

Public Key :-

$$Y_A = \alpha^{X_A} \bmod q \qquad Y_B = \alpha^{X_B} \bmod q$$
$$= 3^{97} \bmod 353 \qquad = 3^{233} \bmod 353$$

Secret Key :-

$$K = Y_B^{X_A} \bmod q \qquad K = Y_A^{X_B} \bmod q$$

Date

b.) Diffie-Hellman key exchange using prime 47 & generator 11.
Alice chooses secret 9 & Bob chooses secret 16.

$q = 47,\ \alpha = 11,\ X_A = 9,\ X_B = 16$

Generate public key:- $Y_A = \alpha^{X_A} \bmod q$

$= 11^9 \bmod 47$

$= [(11^2 \bmod 47) \times (11^4 \bmod 47) \times (11^2 \bmod 47) \times (11 \bmod 47)] \bmod 47$

27 37 27 11

$= (37 \times 27 \times 27 \times 11) \bmod 47$

$= 39$

$Y_B = \alpha^{X_B} \bmod q = 11^{16} \bmod 47 = 3$

Generate Secret key :-

$K = Y_B^{X_A} \bmod q = 3^9 \bmod 47 = 37$ $\quad K = Y_A^{X_B} \bmod q = 39^{16} \bmod 47 = 37$

$K = 37$

Date

Q.4.a $p=23, q=5$

$p=23$, $\alpha=5$, $X_A=2$, $X_B=3$

randomly generate

Public Key :-

$Y_A = \alpha^{X_A} \bmod p = 5^2 \bmod 23 = 2$ $\quad Y_B = \alpha^{X_B} \bmod p = 5^3 \bmod 23 = 10$

Secret Key :-

$K = Y_B^{X_A} \bmod p = 10^2 \bmod 23$
$= 8$

$K = Y_A^{X_B} \bmod p = 2^3 \bmod 23$
$= 8$

$K = 8$

b.) $p=11$, $\alpha=2$, $X_A=5$, $X_B=12$

Public Key :-

$Y_A = \alpha^{X_A} \bmod p = 2^5 \bmod 11 = 10$ $\quad Y_B = \alpha^{X_B} \bmod q = 2^{12} \bmod 11 = 4$

Secret Key :-

$K = Y_B^{X_A} \bmod p = 4^5 \bmod 11 = 1$ $\quad K = Y_A^{X_B} \bmod 11 = 10^{12} \bmod 11 = 1$

$K = 1$