CP-03

→ Summary of PKI, Digital Certificates & X.509 :-

→ PKI :-

- The entrie system that manages public key cryptography
- It provides everything needed for secure communication on the internet.

⊙ Components of PKI :-

→ Public & Private keys :-
Every system has a key pair publickey & private key.

→ Certificate Authority (CA) :-
It is a trusted organization that issues digital certificates after varifying identity.

→ Registeration Authority (RA) :-
Works under the (CA). varifies user identity before (CA) issues certificate.

→ Certificate Database :-
Stores issued certificates & their status.

→ CRL (certificate Revocation List) / OCSP :-
used to check whether a certificate is revoked.

→ Policies & Procedures :-

rules that define how certificates are issued, used & revoked.

@ Provides:-

It provides confidentiality, integrity, Authentication & non-repudiation.

→ Digital certificates:

It is an electronic document issued by a CA. It act as a digital identity card. It is used to associate a public key with a real identity.

⊙ parts of certificate:

↳ Subject name.

↳ Public key.

↳ issuer name.

↳ validity period.

↳ serial number.

↳ Signature algorithm.

↳ Digital signature of CA.

⊙ purpose of certificate:

verify that public key belongs to trustd person & prevents attacker.

→ What is X.509 :-

It is the standard format for digital certificates.

↳ what fields a certificate must contain.

↳ how it should be structured.

↳ how the CA signs it.

⊙ Structure of an X.509 certificate :-

1- version.

2- serial number.

3- Signature Algorithm.

4- Issuer.

5- validity period.

6- Subject.

7- Subject public key info.

8- Extensions.

9- Signature.

Faiez Tariq
22F-3873
7F

CP#02

→ RSA Algorithm :-

⊙ Book Example :-

Let P = 17 , q = 11 , e = 7 , M = 88

→ key generation :-

•) assume two prime numbers ;

P = 17 , q = 11

•) calculate $n = P \times q$

$n = 17 \times 11 \Rightarrow$ $n = 187$

•) calculate $\phi(n) = (P-1) \times (q-1)$

$\phi(n) = (17-1) \times (11-1) \Rightarrow$ $\phi(n) = 160$

•) Choose value of e : $1 < e < \phi(n)$ & $GCD(e, \phi(n)) = 1$

$\therefore e = 7$

•) calculate $ed \bmod \phi(n) \equiv 1$

Finding d ;

q	r1	r2	r	t1	t2	t = t1 − qt2
22	160	7	6	0	1	−22
1	7	6	1	1	−22	23
6	6	1	0	−22	23	−160
−	1	0	−	(23)		

$d = 23$

•) Private key = $\{d, n\} = \{23, 187\}$

•) Public key = $\{e, n\} = \{7, 187\}$

Isfar Akbar

F228801 Aleena Akram

F219164 Ali Akbar

10:51 AM 12/1/2025

→ Encryption :-

$C = M^e \bmod n$

$C = (88)^7 \% 187$

$C = (88)^3 \cdot (88)^3 \cdot (88)^1$

$C = 88 \cdot 44 \cdot 44$

$C = 170368 \% 187 = 11$

$C = 11$

→ Decryption :-

$M = C^d \bmod n$

$M = (11)^{23} \% 187$

$M = 88$

② Self example :-

let $P = 19$, $Q = 13$, $M = 120$

→ Key generation :-

- $n = P \times Q \Rightarrow (19 \times 13) \Rightarrow n = 247$
- $\phi(n) = (P-1) \times (Q-1) \Rightarrow 18 \times 12 \Rightarrow \phi(n) = 216$
- $e = 5$ ∴ $GCD(5, 216) = 1$
- $ed \bmod \phi(n) \equiv 1$

Q	R1	R2	R	t1	t2	t = t1 − Q·t2
43	216	5	1	0	1	−43
5	5	1	0	1	−43	216
−	1	0	−	−43	216	

-> Public key = [e, n] = [5, 247]
-> Private key = [d, n] = [173, 247]

-> Encryption :-

$C = M^e \bmod n$

$C = (120)^5 \% 247$

$C = 100$

-> Decryption :-

$M = C^d \bmod n$

$M = (100)^{173} \% 247$

$M = 120$

e: using book example key

message = HELLO = [8, 5, 12, 12, 15]

⊙ Encryption :-	⊙ Decryption :-
$H=8 \rightarrow C=(8)^7 \% 187$	$C=46 \rightarrow P=(46)^{23} \% 187$
$C=46$	$8 \rightarrow H$
$E=5 \rightarrow C=(5)^7 \% 187$	$C=99 \rightarrow P=(99)^{23} \% 187$
$C=99$	$5 \rightarrow E$
$L=12 \rightarrow C=(12)^7 \% 187$	$C=85 \rightarrow P=(85)^{23} \% 187$
$C=85$	$12 \rightarrow L$
$L=12 \rightarrow C=(12)^7 \% 187$	$C=85 \rightarrow P=(85)^{23} \% 187$
$C=85$	$12 \rightarrow L$
$O=15 \rightarrow C=(15)^7 \% 187$	$C=13 \rightarrow P=(13)^{23} \% 187$
$C=13$	$15 \rightarrow O$
cipher = [46, 99, 85, 85, 13]	text = [8, 5, 12, 12, 15]