ID: 18DCS007
NAME: RUDRA BARAD
22/02/2021 SUB: CNS

Page No.
Date / /

Q1. Different types of services & mechanism

SERVICES – (I) Data Confidentiality
(II) Data Integrity
↳ Anti Change
↳ Anti Replay
(III) Access control
(IV) Authentication
↳ Peer entity
↳ Data Origin
(V) Non-Reputation
↳ Proof of origin
↳ Proof of delivery

MECHANISM –

(I) Encipherment : Data confidentiality, authentication
↳ Hiding / covering data • Integrity
↳ Cryptography
↳ Stegenography

SERVICES

(II) Data Signature : Integrity, non-repudiation,
↳ Electronically sign data • Authentication
↳ Electronically verify data.

SERVICES

(iii) Data Integrity : Integrity, non-repudiation
↳ data + check value (checksum)

(iv) Traffic Padding : Data confidentiality
↳ bogus data + real data

(v) Notorization : Integrity, Non-repudiation
↳ trusted 3rd party

(vi) Authentication Exchange : Integrity, authentication, non-repudiation, acess control
↳ exchange msg for identity

(vii) Access Control : Access control
↳ provides right to acess data

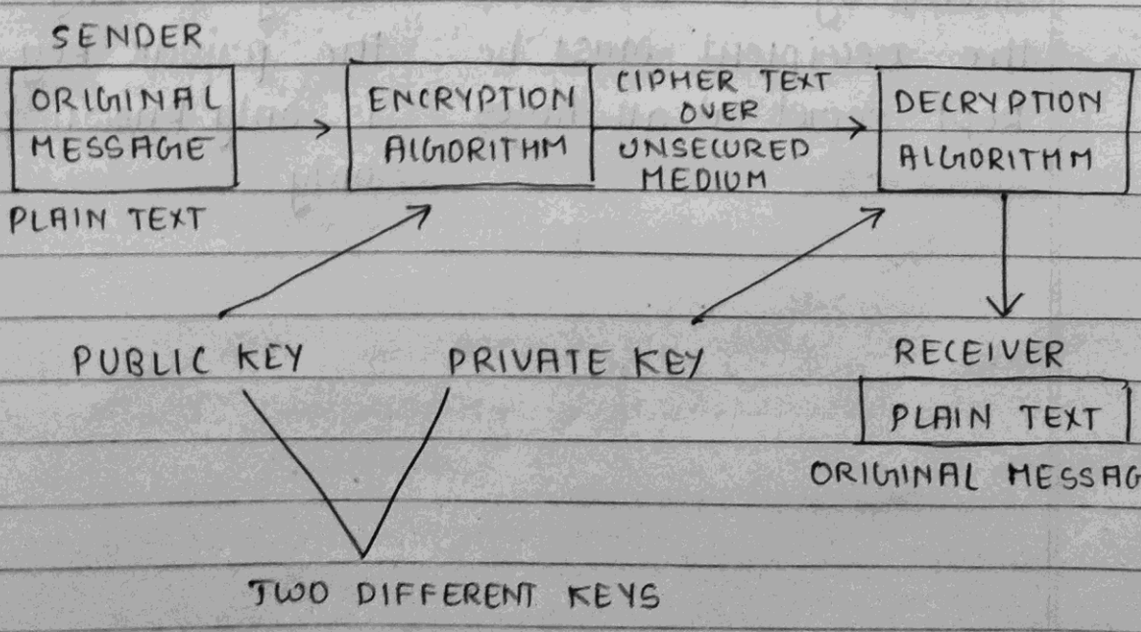
(viii) Routing Control : Data Confidentiality
↳ use of different paths

Page No.
Date / /

Q2.

	ACTIVE ATTACK	PASSIVE ATTACK
→	In the kind of attacks the goal is to make changes on modify data. (attack on integrity & availability	In these kind of attacks the goal is just to obtain the information (attack on confidentiality)
→	Attacks are easy to detect	Attacks are comparatively hard to detect.
→	Attacks are hard to prevent	Attacks are easy to prevent
→	Attacks are intended to harm the system	Attacks are not intended to harm system
→	Eg. DOS, Masquerading	Eg. Snooping, Traffic analysis

Q6.



ID: 18DCS007
NAME: RUDRA BARAD

Pg 4.

Page No.
Date / /

→ In this cryptography, public key is disclosed to all the users in network and private key is secret key known only to a particular user.

→ Private key is never distributed by receivers

→ Public key is used for cryption and private key is used for decryption

	CONVENTIONAL ENCRYPTION	PUBLIC KEY ENCRYPTION
→	It is a type of cryptograph system which uses a single key to both encrypt & decrypt message	type of encryption scheme which instead of single key, uses pair of key to encrypt & decrypt msg.
→	same secret key is shared by the sender & the recipient must be kept secret at all times	public key can be shared freely to anyone while the private key secret & is only known by recipient only

ID 18DCS007
NAME: RUDRA BARAD Pg 5.

Page No.
Date / /

Q10. DIFFIE - HELLMAN KEY EXCHANGE ALGORITHM

We are given two prime no. $n = 11$
$g = 19$

Alice private number, $x = 3$
Bob private number, $y = 6$

Now $A = g^x \bmod n$
$= 19^3 \bmod 11$
$= 6859 \bmod 11$
$= 6$

Alice will send this A to Bob

Similarly $B = g^y \bmod n$
$= 19^6 \bmod 11$
$= 3$

Bob will send this B to Alice
Now, secret key

$K_1 \rightarrow B^x \bmod n$
$3^3 \bmod 11 = 5$ $\boxed{K_1 = 5}$

$K_2 \rightarrow A^y \bmod n$
$6^6 \bmod 11 = 5$ $\boxed{K_2 = 5}$

Therefore we see $\boxed{K_1 = K_2} = K = 5$

ID: 18DCS007
NAME: RUDRA BARAD

Page No.
Date / /

Q9. Different attacks on RSA

Q7.

(i) FACTORIZATION
(ii) CHOSEN - CIPHERTEXT
(iii) ENCRYPTION EXPONENTS - copper smith
- broad cast
- related messages
- short pad

(iv) DECRYPTION EXPONENT - Revoked & low exponents
(v) PLAIN TEXT - this is potential attack on
- Short messag1
- cyclic & unconcealed

(vi) MODULUS - common modulus
(vii) IMPLEMENTATION - timming
- power

→ In chosen ciphertext the attacker can find out the plain text from ciphertext using extended euclideon algo

→ In factorization the attacker impersonates the key avenue & with the help of stolen cryptographic data, they decryp sensitive data, bypass the securely of system.

Page No.
Date / /

Q7. Two prime numbers are 17 & 11
Public key = 13

$N = 17 \times 11$
$= 187$

$\phi(n) = 16 \times 10 = 160$
Public key = 13

Here, let d be a private key
$(d \times 13) \bmod 160 = 1$

Inverse of 13

Q	R1	R2	R	T1	T2	t
12	160	13	4	0	1	-12
3	13	4	1	1	-12	37
4	4	1	0	-12	37	-160
	1	0		37	-160	

PRIVATE KEY = 37

ID: 18DCSD07
NAME: RUDRA BARAD

(8)

Page No.
Date / /

Q4. Suppose CIPHERTEXT = C, PLAINTEXT FP = P, KEY = K

LHS = At receiver's side ciphertext
= C
= (P × K) mod 26 (∵ multiplication cipher)
= ((C × K⁻¹) × K) mod 26 (∵ P = C × K⁻¹ mod 26)
= (C × K⁻¹ × K) mod 26
= C mod 26
= C
= At senders side
= RHS

Q3. (i) REPLAYING - because same activity is repeated
(ii) DOS - denial of service because server is unavailable

Q8. RSA Algorithm is most populous asymmetric key cryptographic algorithm.

WORKING:

1. Choose any 2 larger prime no say A & B
2. calculate N = A * B
$\phi(n) = (A-1) * (B-1)$
3. calculate $\phi(n)$, choose public key E such that it is not a factor of $\phi(n)$
4. Select private key D that matches following condition
$(D * E) \bmod \phi n = 1$

Page No.
Date / /

6. For encryption = ciphertext = $P^c \bmod n$

7. For decryption = $PT = CT^d \bmod n$

→ The reason prime nos are fundamental to RSA enc is because when you multiply togethe the result is a no. that can only be broken down into those primes

Page No.
Date / /

Qs. PLAINTEXT = "ST"
CIPHERTEXT1 = "CG"
CIPHERTEXT2 = "SD"

(1) ST → CG

S → C	T → G
18 → 2	19 → 6

Now eqn for affine cipher

$$P \times K_1 + K_2 = C \bmod 26$$
$$18K_1 + K_2 = 2 \pmod{26}$$
$$19K_1 + K_2 = 6 \pmod{26}$$

$$\begin{bmatrix} 18 & 1 \\ 19 & 1 \end{bmatrix} \begin{bmatrix} K_1 \\ K_2 \end{bmatrix} = \begin{bmatrix} 2 \\ 6 \end{bmatrix} \bmod 26$$

$$\begin{bmatrix} K_1 \\ K_2 \end{bmatrix} = \begin{bmatrix} 18 & 1 \\ 19 & 1 \end{bmatrix}^{-1} \begin{bmatrix} 2 \\ 6 \end{bmatrix} \bmod 26$$

$$= \frac{1}{-1} \begin{bmatrix} 18 & 1 \\ 19 & 1 \end{bmatrix}^{-1} \begin{bmatrix} 2 \\ 6 \end{bmatrix} \bmod 26$$

$$= \frac{1}{25} \begin{bmatrix} 1 & -1 \\ -19 & 18 \end{bmatrix} \begin{bmatrix} 2 \\ 6 \end{bmatrix} \bmod 26$$

Inverse for 25 in Z_26

Q	R1	R2	R	T1	T2	T
1	26	25	1	0	1	-1
25	25	1	0	1	-1	26
	1	0		-1	26	

Inverse = -1+26
= 25

$$= 25 \begin{bmatrix} 1 & 25 \\ 7 & 18 \end{bmatrix} \begin{bmatrix} 2 \\ 6 \end{bmatrix}$$

$$= \begin{bmatrix} 25 & 625 \\ 175 & 450 \end{bmatrix} \begin{bmatrix} 2 \\ 6 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 50 + 3750 \\ 350 + 2700 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 3800 \\ 3050 \end{bmatrix} \bmod 26$$

$K_1 = 4$ $K_2 = 8$

Here K_1 is not possible as GCD $(K_1, 26) \neq 1$

(11) ST → SD

S → S	T → D
18 → 18	19 → 3

Now, $18K_1 + K_2 = 18 \pmod{26}$
$19K_1 + K_2 = 3 \pmod{26}$

Page No.
Date / /

$$\begin{bmatrix} 18 & 1 \\ 19 & 1 \end{bmatrix} \begin{bmatrix} K_1 \\ K_2 \end{bmatrix} = \begin{bmatrix} 18 \\ 3 \end{bmatrix} \bmod 26$$

$$\begin{bmatrix} K_1 \\ K_2 \end{bmatrix} = \begin{bmatrix} 18 & 1 \\ 19 & 1 \end{bmatrix}^{-1} \begin{bmatrix} 18 \\ 3 \end{bmatrix} \bmod 26$$

$$= \frac{1}{-1} \begin{bmatrix} 1 & -1 \\ -19 & 18 \end{bmatrix} \begin{bmatrix} 18 \\ 3 \end{bmatrix} \bmod 26$$

$$= \frac{1}{25} \begin{bmatrix} 1 & 25 \\ 7 & 18 \end{bmatrix} \begin{bmatrix} 18 \\ 3 \end{bmatrix}$$

= Since inverse of 25 is "25" as done before

$$= 25 \begin{bmatrix} 1 & 25 \\ 7 & 18 \end{bmatrix} \begin{bmatrix} 18 \\ 3 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 25 & 625 \\ 175 & 450 \end{bmatrix} \begin{bmatrix} 18 \\ 3 \end{bmatrix}$$

$$= \begin{bmatrix} 2325 \\ 4500 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 11 \\ 2 \end{bmatrix}$$

This key is valid, since $K_1 = 11$ 8
inverse of K_1 is in Z^*26

CIPHERTEXT = "JULSDCH"

Page No.
Date / /

(i) For J $= (C - K_2) K^{-1} \bmod 26$
$= (9 - 2) 11^{-1} \bmod 26$

By similar method of table $= 19$

$= (7)(19) \bmod 26$
$= 133 \bmod 26$
$= 3 = D$

(ii) For U $= (20 - 2) 19 \bmod 26$
$= 4 = E$

(iii) For L similarly $\Rightarrow P$

(iv) For S similarly $\Rightarrow S$

(v) For D similarly $\Rightarrow T$

(vi) For C similarly $\Rightarrow A$

(vii) For H similarly $\Rightarrow R$

ORIGINAL TEXT = DEPSTAR