Amit K. Wernekar

VIT Vidyalankar Institute of Technology
(Accredited A+ by NAAC)
(Autonomous Institute Affiliated to University of Mumbai)

Mid Semester Examination

Branch	Date	Sem.	Roll No. / Exam Seat No.	Subject	Student's Signature	Junior Supervisor's Name and Sign
CMPN	8/2	5		CSS-1		

Question No.	A	B	C	D	E	F	G	H	Total	Total out of (20 /30 / 40)
1										
2										
3										
4										

Examiners Signature	Student's Sign (After receiving the assessed answer sheet)

Q1

a. Form a rectangle & take horizontal opposite letter.

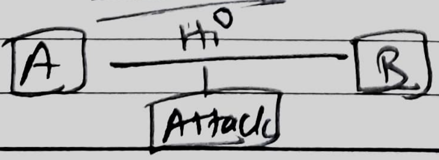
b. Authentication: Validation of user

Authorization: Verification of user Rights.

c. End to Encryption:

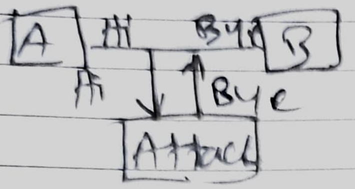
It while sending converts plaint to ciphertext & while receiving converts cipher to plain text

d. ~~Eos~~ Interception



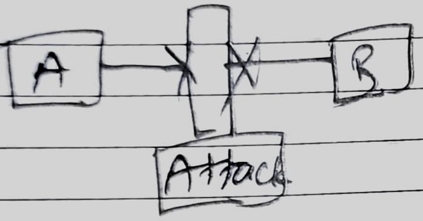
Loss of integrity

Modification



loss of Integrity

Interruption



Loss of availability.

e. Client verifies dijital signature of CA using CA's publick key.

f. 3 D's of security

① Defence

② Detect

③ Deterrence

g. Ransomware attack.

h. VIDYLANKAR K=3

P.T.	V	I	D	Y	L	A	W	K	A	R
Pos.	21	8	3	24	11	0	13	10	0	17
Key	3	3	3	3	3	3	3	3	3	3
PTK	24	11	6	27	14	3	16	13	3	20
PTK%26	24	11	6	~~27~~1	14	3	16	13	3	20
C.T.	Y	L	G	B	O	D	Q	N	D	U

Q2

a Keyless transposition for k=3

TECOMPUTERENGG

T				M				E				G	
	E		O		P		T		R	.	N		G
		C				U			E	E			

TMEGEOPTRNGCUE

Decryption

I	T				M				E				G	
II		E		O		R		T		R		N		G
III			C				U				E			

∴ TECOMPUTERENGG.

Q2

b Euclid's algorithm

It is a recursive GCD finding method:

```
int GCD(int x, int y)
{
   if(y==0)
      return x;
   else
      ~~return(y, x%GCD(x%y~~
      return GCD((y,x%y);
   }
}
```

eg GCD($\overset{105}{\cancel{80}}$, $\overset{80}{\cancel{105}}$)

= GCD (80, 105 mod 80 = 25)

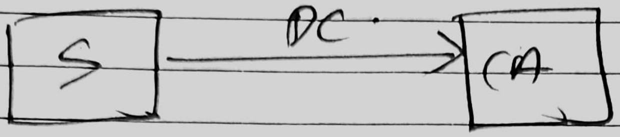
= GCD(25, 80 mod 25 = 5)

= GCD(5, 25 mod 5 = 0)

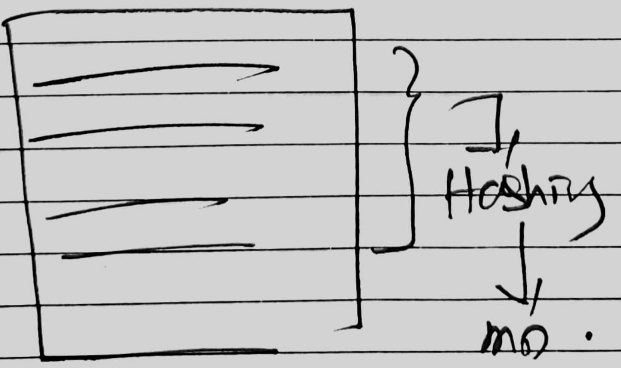
= GCD(5, 0)

$\therefore \boxed{\text{GCD} = 5}$

Q3a



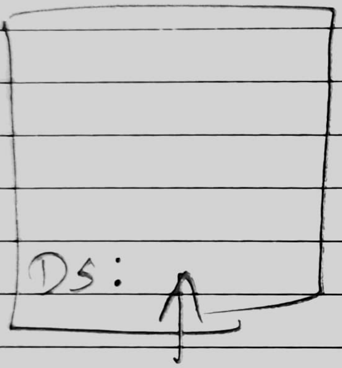
- Server Creates the Digital certificate by putting IP, MAC, publickey, Port & URL.
- It then encrypts the D.C. using Server's Private key. & Send it to CA.
- CA [certification authority] decrypts the received message i.e D.C. using servers Public key, if decrypted successfully then Server is validated.
- CA now verifies all the details of the ~~CA~~ Server as mentioned in the DC.
- If valid then:



CA applies hashing on the entire D.C. which gives MD [message Digest].

MD —— Enc. using CA'S private key —— D.S.

Now CA encrypts MD using the CA'S private key & gets the Digital signature.



DS is now put at the end & this digitally signed certificate is sent to server.

$\boxed{CA} \xrightarrow{DSC} \boxed{S}$

Q 3 b RSA algorithm to create Digital Signature:

(1) Select two large prime numbers p & q

(2) Compute $n = p * q$

(3) Compute $\phi(n)$

$\therefore \phi(n) = \phi(p) * \phi(q)$

$\because$ p & q are prime $\therefore$ $\phi(p) = p-1$
$\phi(q) = q-1$

(4) Now select a publick key e such that

(1) $0 \leq e \leq \phi(n)$

(2) $GCD(e, \phi(n)) = 1$

(5) Calculate the private key d

$$\boxed{\begin{array}{l} d \equiv e \bmod \phi(n) \\ \Rightarrow de^{-1} \bmod \phi(n) = 1 \end{array}}$$

(6) Public key (e, n)

Private key (d, n)

7 Create Digital Signature

$$DS = m^d \bmod n$$

8 Verify Digital signature

$$M' = DS^e \bmod n.$$

M & M' should be same