Date - 25/2/2

Name: Rajasree Laha
Roll: CSE2/14002
Course Title: Cryptography & Network Security
Course code: CSEUGPC26
Sem: 8th   year: 4th
Dept: CSE

Date = 25/7/25

INDEX

Sl. no.	Question	Output	Date	Teacher's Signature
1	P.T : Today is Tuesday, Keyword : AX2. Use vigenere cipher to convert P.T into C.T	C.T: TLCABHSG TEPCAB	5/2/25	
2 a)	Key: NICKS, PT: ALIAH UNIVERSITY. Use single Columnar to Convert P.T to C.T.	C.T: IITLNSAVT AURHEY	5/2/25	
3	Using the RSA algo encrypt & decrypt the message : BE, with key pairs (3,15) & (3,15)	Encryption message: 8 5 Decryption message: BE	4/3/25	
4	Explain how integrity, non-repudiation, authentication are achieved by using digital signature.	written	22/4/25	
5	Assume $h=7$, $n=23$; choose $x=3$, $y=6$, find R_1, R_2 & K_1, K_2.	$R_1=21$, $R_2=4$, $K_1=18$, $K_2=18$	25/4/25	
6	Explain vigenere cipher & rail fence cipher with examples.	written	12/5/25	
7	Explain IPSec Protocol in details.	written	12/5/25	
2 b)	Use singular columnnar transposition cipher on P.T : TODAY IS TUESDAY ; key: NICKS	C.T: DTAOSDA UYTISYE	12/5/25	

Date = 25/2/23

Assignment ①

1) P.T : Today is Tuesday
Keyword: AX2
Use vigenere cipher to convert P.T into C.T.

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

P.T:	T	O	d	a	y		i	s		T	u	e	s	d	a	y									
Key:	A	X	2	A	X	2	A		X	2	A	X	2	A	X										
C.T:	T	L	C	A	B	H	S		Q	S	T	E	P	C	A	B									

Encryption: $(P_i + K_i) \bmod 26$ (E_i)

$E_T = (19+0) \% 26 = 19 \rightarrow T$
$E_O = (14+23) \% 26 = 11 \rightarrow L$
$E_d = (3+25) \% 26 = 2 \rightarrow C$
$E_a = (0+0) \% 26 = 0 \rightarrow A$
$E_y = (24+23) \% 26 = 1 \rightarrow B$
$E_i = (8+25) \% 26 = 7 \rightarrow H$
$E_s = (18+0) \% 26 = 18 \rightarrow S$
$E_T = (19+23) \% 26 = 16 \rightarrow Q$
$E_u = (20+25) \% 26 = 19 \rightarrow T$
$E_e = (4+0) \% 26 = 4 \rightarrow E$
$E_s = (18+23) \% 26 = 15 \rightarrow P$
$E_d = (3+25) \% 26 = 2 \rightarrow C$
$E_a = A$
$E_y = B$

Date = 4/3/25

② Key: NICKS

a) P.T: ALIAH UNIVERSITY

Use single columnar to convert P.T into C.T.

N	I	C	K	S
4	2	1	3	5
A	L	I	A	H
U	N	I	V	E
R	S	I	T	Y

C.T: IITLNSAVTAURHEY

b) Use singular columnar transposition cipher on:

P.T: TODAY IS TUESDAY

Key: NICKS

N	I	C	K	S
4	2	1	3	5
T	O	D	A	Y
I	S	T	U	E
S	D	A	Y	

C.T: DTAOSDAUYTISYE

Date = 4/3/25

(3) Using the RSA algo encrypty & decrypt the message : BE, with key pairs (3, 15) & (5, 15).

P.T = BE

N = 15, e = 3, d = 5

(3, 15) ↓ Public key (encryption)

(5, 15) ↓ Private key (decryption)

For B,

encryption, [C = C.T.]

$C = (2)^3 \% 15$ [B = P = 2]

$= 8$ [P = P.T.]

$\boxed{C = 8}$

For E encryption [C = C.T.]

$C = (5)^3 \% 15$ [P = E = 5]

$= 5$ [P = P.T.]

$\boxed{C = 5}$

∴ Encrypted message 8, 5

For B decryption,

$P = (8)^5 \% 15$

$= 2$ (= B)

For E decryption,

$P = (5)^5 \% 15$

$= 5$ (= E)

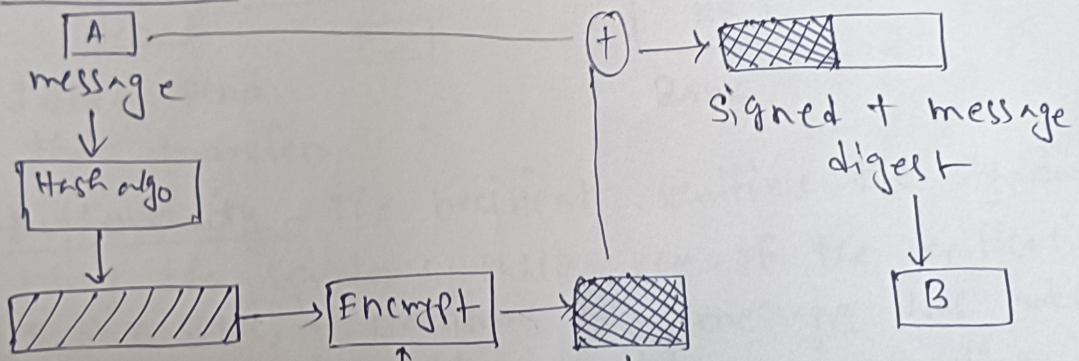
∴ the decrypted message is 'BE' (we should get BE as decrypted message otherwise the calculation is wrong, as we had encrypted BE as 8, 5 so the decryption of 8 5 must give BE).

Date = 23/4/25

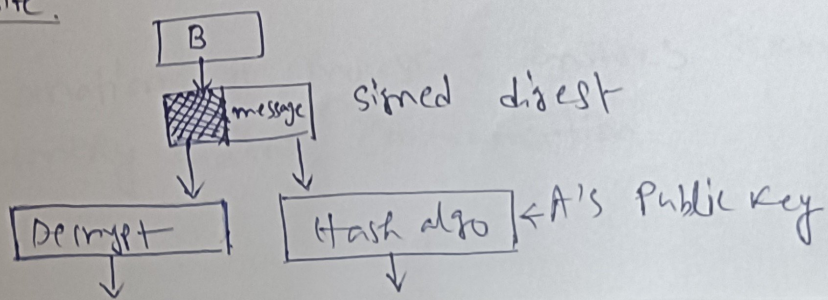
(4) Explain how integrity, non-repudiation, authenticity are achieved by using digital signature.

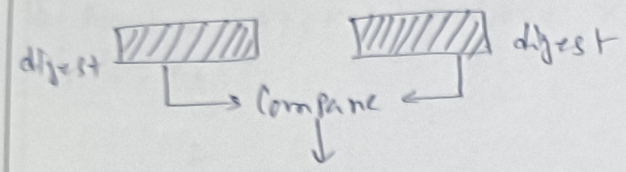
Integrity - When a sender creates a digital signature, they first generate a hash (a fixed length representation) of the original message. This hash is then encrypted with their private key to create the signature. On the receiving end, the recipient decrypts the signature using the sender's public key & compares the resulting hash with a newly generated hash of the received message. If they match, the message has not been altered.

Sender's site:



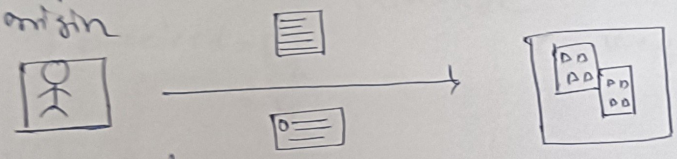
Receiver's site:





If Same then accept

Non-repudiation - only the sender has access to their private key. Because the signature is created using this key, the sender can't later deny having signed the message, as no one else could have created that exact signature.



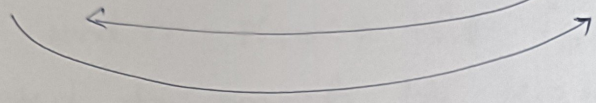
Authenticity - The recipient verifies the signature using the sender's public key. If the verification is successful, it confirms the message was indeed signed by the holders of the corresponding private key - authenticating the sender's identity.

This combination of processes ensures secure & trustworthy digital communication.

Date = 25/4/25

⑤ Assume G=7, N=23; chose x=3, y=6; find R_1, R_2 & K_1, K_2.

A	B
Key generated = $R_1 = G^x \bmod N$	Key generated = $R_2 = G^y \bmod N$
$= 7^3 \bmod 23$	$= 7^6 \bmod 23$
$= 21$	$= 4$.
Key received = R_2	Key received = R_1
$= 4$	$= 21$
Secret Key = K_1	Secret key = K_2
$= R_2^x \bmod N$	$= R_1^y \bmod N$
$= 4^3 \bmod 23$	$= 21^6 \bmod 23$
$= 18$	$= 18$



$\therefore K_1 = K_2$

$\therefore R_1 = 21$, $R_2 = 4$, $K_1 = 18$, $K_2 = 18$.

Date = 12/5/25

⑥ Explain vigenere cipher & rail fence cipher with examples. vigenere cipher

The vigenere cipher is a method of encrypting alphabetic text using a series of caesar cipher based on the letters of a keyword. It's also called polyalphabetic cipher.

Working -

i) Plaintext - The original message we want to encrypt.

ii) Key - A word or phrase that is repeated/truncated to match the length of the plain text.

iii) Encryption process -

a) Each letter in the plain text is shifted by a no. of positions defined by the corresponding letter in the key.

b) For eg, if the P.t. letter is A, & the key letter is C, then A is shifted 2 positions forward to C.

Advantages - Harder to crack than a caesar cipher due to the multiple shifting.

Disadvantages - If the key is short, it becomes vulnerable to frequency analysis.

Example -

P.T : GEEKSFORGEEKS

Keyword: AYUSH

G E E K S F O R G E E K S
A Y U S H A Y U S H A Y U

encryption,

encryption
$E_i = (P_i + K_i) \bmod 26$

$E_G = (6+0) \bmod 26 = 6 \rightarrow G$
$E_E = (4+24) \bmod 26 = 2 \rightarrow C$
$E_E = (4+21) \bmod 26 = 25 \rightarrow Z$
$E_K = (10+18) \bmod 26 = 2 \rightarrow C$
$E_S = (18+7) \bmod 26 = 25 \rightarrow Z$
$E_F = (5+10) \bmod 26 = 5 \rightarrow F$
$E_O = (14+24) \bmod 26 = 12 \rightarrow M$
$E_R = (17+20) \bmod 26 = 10 \rightarrow K$
$E_G = (6+18) \bmod 26 = 24 \rightarrow Y$
$E_E = (4+7) \bmod 26 = 11 \rightarrow L$
$E_E = (4+0) \bmod 26 = 4 \rightarrow E$
$E_K = (10+24) \bmod 26 = 8 \rightarrow I$
$E_S = (18+21) \bmod 26 = 13 \rightarrow N$

∴ G E E K S F O R G E E K S ← (Plain text)
| | | | | | | | | | | |
G C Z C Z F M K Y L E I N ← (Cipher text)

decryption, Just Substract the key's letter value instead of adding we'll get GEEKSFORGEEKS again. (from GCZCZFMKYLEIN (if doing from it)).

decryption
$D_i = (E_i - K_i) \bmod 26$

Rail fence cipher

It's a type of transpontation cipher, which means it rearranges the characters of the main text to form the ciphertext, without changing the actual letters.

Working

i) Choose a no. of 'rails' (rows), e.g. 3
ii) Write the message in a zigzag pattern across the rails.
iii) Read off each row to get the ciphertext.

Decryption -

i) Determine how many characters go in each row.
ii) Fill the rows with the ciphertext.
iii) Rebuild the original zigzag to extract the P.t.

Advantages - Simple & fast to implement, suitable for basic obfuscation.

Disadvantages - Easily breakable with Pattern analysis / brute force due to Predictable structure.

Example

P-T - GEEKSFORGEEKS, key value = 2

∴ G E S O G E S
  E K F R E K S

∴ C.t - GESOGESEKFREK

(7) Explain IPSec Protocol in details.

IPSec (Internet protocol security) is a suite of protocols used to secure IP communication by authenticating & encrypting each IP packet in a data stream.

Features / characteristics

i) Confidentiality - Encrypts data to keep it private.
ii) Integrity - Ensures data hasn't been altered.
iii) Authentication - verifies the identity of the sender.
iv) Anti-replay - Prevents attackers from resending packets.

main components -

i) Protocols - i) AH (Authentication header), that provides authentication & integrity.
ii) ESP (Encapsulating security payload), that provides encryption, authentication & integrity.

ii) modes -

a) transport mode - Encrypts only the data (payload) of the IP packet.
b) Tunnel mode - Encrypts the entire IP packet & wraps it in a new one (used in VPN's).

iii) key exchange -

Uses IKE (Internet key exchange) to

establish & manage security associations (SAs).

Use case / Example - It is commonly used in VPNs (virtual private networks) to create secure tunnels over the internet.