Question 1 [25 Marks]

[CLO 3: Apply various security and risk management tools for achieving information security and privacy]

Fill in the blanks in the space provided and write working on the last page (extra work/calculations).

a) A captured encrypted message is suspected to be encrypted using Rail Fence 3 rails (depth=3): **[5 marks]**

WECRLTEERDSOEEFEAOCAIVDEN

Fill in rail positions (just first few letters):

W E C R L T E E R D S O E F E A O C A I V D E N

T E E R D S O F

F E A

Rail 1: W _ _ L _ _ E _ _ S _ _

Rail 2: _ E C _ T E _ R D _ E _

Rail 3: _ _ R _ E _ O _ E _ A _

Recovered plaintext: ~~WECR~~ ~~WE~~ WTEEEEF

b) Columnar Transposition Cipher (Decryption) **[5 marks]**

An employee receives the following ciphertext that was encrypted using Columnar Transposition.

The keyword used is LOCKED.

Keyword order (write numeric order under each letter):

L	O	C	K	E	D
5	6	1	4	3	2

Ciphertext: ØFRXUYAXLRXXDOEXGCOMOKUS

Step 1 - Write ciphertext in the blanks given below to decrypt:

L	O	C	K	E	D
Ø	F	R	X	U	Y
A	X	L	R	X	E
Q	O	E	X	G	C
O	M	Q	K	U	S
-	-	-	-	-	-
-	-	-	-	-	-
C	D	E	H	L	O

A
B
C -1
D -2
E -3
F
G
H
I
J
K -4
L -5
M
N
O
P -6
Q
R
S
T
U
V

National University of Computer and Emerging Sciences
Islamabad Campus

Step 2 - Write down the plaintext in the blank given below

Plaintext: RVUXOF LXXRAX ECGXDO OSUKOM

c) Frequency Analysis [5 marks]

A cybersecurity analyst intercepts an encrypted message suspected to be encrypted using a monoalphabetic substitution cipher. The ciphertext is shown below:

NGXIQCTFGZSGGATRZITDTLLQUT

The analyst performs frequency analysis on the ciphertext and observes the following clues:

Cipher Letter	Frequency	Notes
T / L	High	Likely maps to E or T (most common English letters)
Z	Medium	Often maps to A or T
U	Medium	Possible O or A
N / G / X	Low	Likely consonants

Additional hint: The sentence appears to be a normal English statement.

Tasks

1. **Using the frequency hints and common English patterns, identify likely plaintext words in the sentence.**
2. **Fill in the partially-decoded plaintext below (letters revealed as hints):**
   NGX IQCT FGZ SGGATR ZIT DTLLQUT
   FOR GAME BOT COOKED TIE JESSALE
   B C D
3. **Write the final decrypted plaintext sentence below:**

Plaintext: FOR GAME BOT COOKED TIE JESSALE

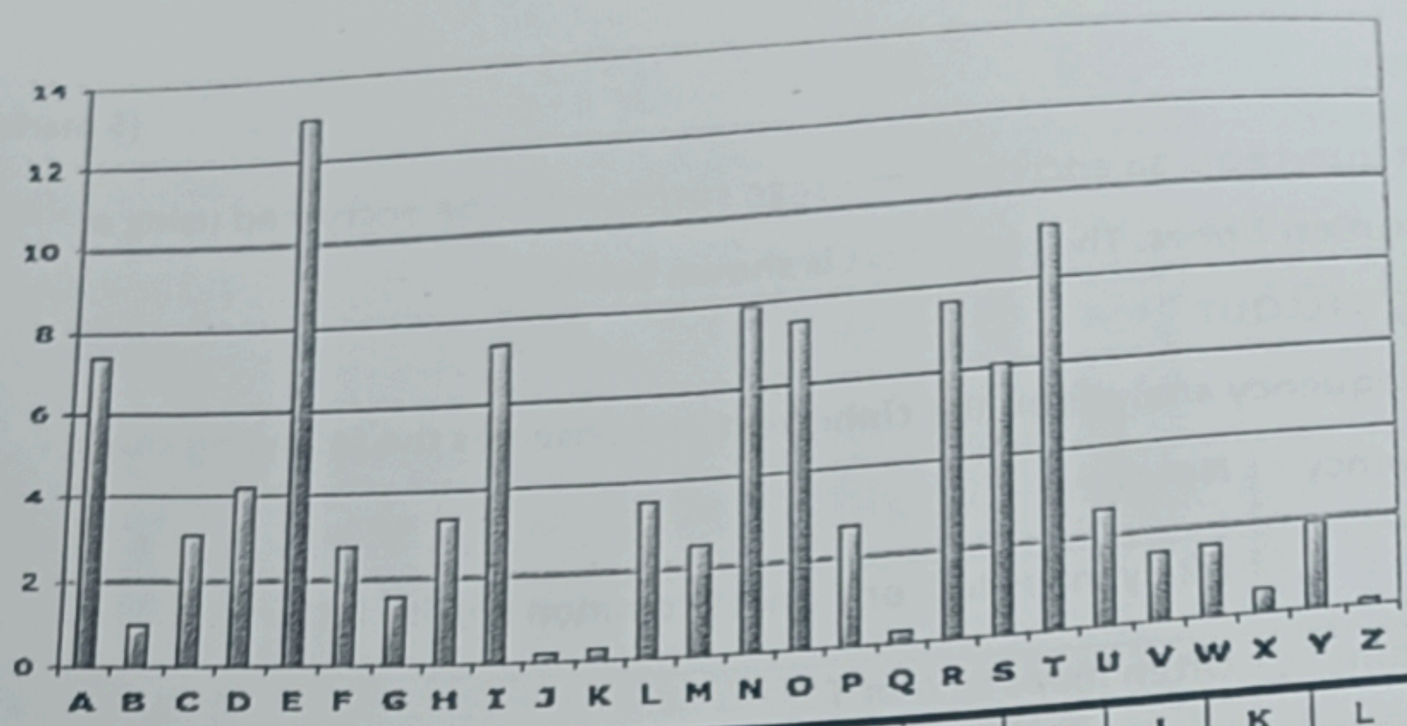
G - O

A
B
C
D
E
F
G
I
K
M
O
R
S
T

H
J
L
N
P
Q
U
V
W
X
Y
Z

National University of Computer and Emerging Sciences

Islamabad Campus



Letter	A	B	C	D	E	F	G	H	I	J	K	L	M
Frequency	7.4	1.0	3.1	4.2	13.0	2.8	1.6	3.4	7.4	0.2	0.3	3.6	2.5
Letter	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Frequency	7.9	8.0	2.7	0.3	8.0	6.1	9.2	2.6	1.5	1.6	0.5	1.9	0.1

d) ***In the AES-128 encryption algorithm, each round (except the last) includes a MixColumns transformation. You are given the following state matrix (in hexadecimal) before MixColumns:***

$$\text{State} = \begin{bmatrix} D4 & E0 & B8 & 1E \\ BF & B4 & 41 & 27 \\ 5D & 52 & 11 & 98 \\ 30 & AE & F1 & E5 \end{bmatrix}$$

and the MixColumns transformation matrix:

$$M = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix}$$

Compute only the 2nd byte of 3rd word after the MixColumns transformation.

Fill in the blanks and show your working on last page: **[5 marks]**

$b'_{(3,4)} = (\underline{1} \times \underline{B8}) \oplus (\underline{2} \times \underline{41}) \oplus (\underline{3} \times \underline{11}) \oplus (\underline{1} \times \underline{F1})$

National University of Computer and Emerging Sciences
Islamabad Campus

= B8 ⊕ 82 ⊕ 33 ⊕ F1

= F8

e) You are given the following AES key schedule words (in hexadecimal): [5 marks]

$$\text{Key Words } (W_0\text{–}W_7) = \begin{bmatrix} 2B & 28 & AB & 09 & A0 & 88 & 23 & 2A \\ 7E & AE & F7 & CF & FA & 54 & A3 & 6C \\ 15 & D2 & 97 & 4F & FE & 2C & 39 & 76 \\ 16 & A6 & 75 & 3C & 17 & B1 & 39 & 05 \end{bmatrix}$$

Rcon Matrix (Round Constants)

$$\text{Rcon} = \begin{bmatrix} 01 & 02 & 04 & 08 & 10 & 20 & 40 & 80 & 1B & 36 \\ 00 & 00 & 00 & 00 & 00 & 00 & 00 & 00 & 00 & 00 \\ 00 & 00 & 00 & 00 & 00 & 00 & 00 & 00 & 00 & 00 \\ 00 & 00 & 00 & 00 & 00 & 00 & 00 & 00 & 00 & 00 \end{bmatrix}$$

Using the AES-128 key expansion process, compute the next two words:

W_8 and W_9.

W_8 = _____

W_9 = _____

x \ y	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
6	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
8	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
A	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
B	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
C	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
D	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
E	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
F	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

(a) S-box

Question 2 [25 Marks]

To be answered on the last page

[CLO 1: Explain key concepts of information security such as design principles, cryptography, risk management]

1. **In DES, during the Feistel function (f-function), the 32-bit right half is expanded to 48 bits using: [1 mark]**
   - a. Initial Permutation (IP)
   - b. Key Schedule (PC-1)
   - c. Expansion D-box (E)
   - d. Substitution Boxes (S-boxes)

2. **Given $p = 61$, $q = 53$, and $e = 17$. Find the modulus n and Euler's totient $\varphi(n)$. [2 marks]**
   - a. $n = 3233$, $\varphi(n) = 3120$
   - b. $n = 3120$, $\varphi(n) = 3233$
   - c. $n = 3233$, $\varphi(n) = 3180$
   - d. None of above

   $n = p * q$ $\quad \phi(n) = (p-1)*(q-1)$
   $= 61 * 53$ $\quad = 60 \times 52$
   $= 3233$ $\quad =$

3. **For the same RSA setup, find the private exponent d such that $17 \cdot d \equiv 1 \pmod{3120}$. [2 marks]**
   - a. 157
   - b. 2753
   - c. 187
   - d. None of above

   $p = 61 \quad q = 53 \quad e = 17$
   $\phi(n) = 3120 \quad n = 3233$
   $17.d \mod (3120) = 1$
   $\Rightarrow \quad \frac{3120 * 0 + 1}{17} = d$

4. **After XORing the expanded right half with the round key, which of the following steps reduces the data back to 32 bits? [1 mark]**
   - a. P-box permutation
   - b. Key mixing
   - c. S-box substitution
   - d. Left circular shift

   2669
   6.599×10^{30}
   46800.
   6.599×10^{30}
   2×10^{27}
   2×10^{27}

5. **Encrypt $m = 65$ using the public key ($n = 3233$, $e = 17$). Find ciphertext $c \equiv m^{17} \pmod{3233}$. [2 marks]**
   - a. 2790
   - b. 2805

   $65^{17} \mod 3233$

c. 2753

d. None of above

6. Given $n = 2773$, $e = 17$, $d = 157$, and ciphertext $c = 1924$, find the plaintext message m. [2 marks]

a. 65

b. 157

c. 123

d. None of above

n = 2773 e = 17 d = 157 c = 1924

$1924^{d} \bmod n$ $\quad C = m^{e} \bmod m$

$1924^{157} \bmod 2773$ $\quad 65^{17} \bmod 2773$

7. Which of the following correctly describes one round of DES encryption? [2 marks]

a. $L_i = R_{i-1}, \quad R_i = L_{i-1} \oplus f(R_{i-1}, K_i)$

b. $R_i = L_{i-1}, \quad L_i = R_{i-1} \oplus f(L_{i-1}, K_i)$

c. $L_i = f(R_{i-1}, K_i), \quad R_i = L_{i-1}$

d. $L_i = L_{i-1}, \quad R_i = f(R_{i-1}, K_i)$

8. The DES key schedule starts with a 64-bit key, but only 56 bits are used because: [1 mark]

a. The remaining 8 bits are for parity checking.

b. The remaining 8 bits are discarded for security reasons.

c. The 8 bits are added to the IV (Initialization Vector).

d. They are used in the expansion step.

8. Let $p = 23$, $g = 5$, $a = 6$, $b = 15$. Find the shared secret s after both parties exchange their public keys. [2 marks]

a. 8

b. 5

c. 19

d. None of above

p = 23
g = 5 a = 6 b = 17

$g^{5} \bmod 23$

a & b are private keys or what?

or use generally accepted notation.

9. In the key generation process, PC-2 (Permutation Choice 2) selects bits from: [1 mark]

a. The output of the Expansion D-box

b. The output of PC-1 after left shifts

c. The plaintext halves (L and R)

d. The ciphertext feedback loop

[CLO 4: Identify appropriate techniques to tackle and solve problems of real life in the discipline of information security]

Analyze the following Cryptographic Flow / Functional Block Diagrams to determine which of the five security properties are provided: Confidentiality (C), Integrity (I), Authentication (A), Non-repudiation (NR), and Freshness (F) (replay safety). For each system:

- **Understand what remains [Private] and what is exchanged on [Public] channel/ out-of-band [OOB].**
- **Evaluate resistance to MITM and Replay Attack. Then choose the most accurate option.**

C: Information is accessible only to authorized entities (control of keys/credentials).

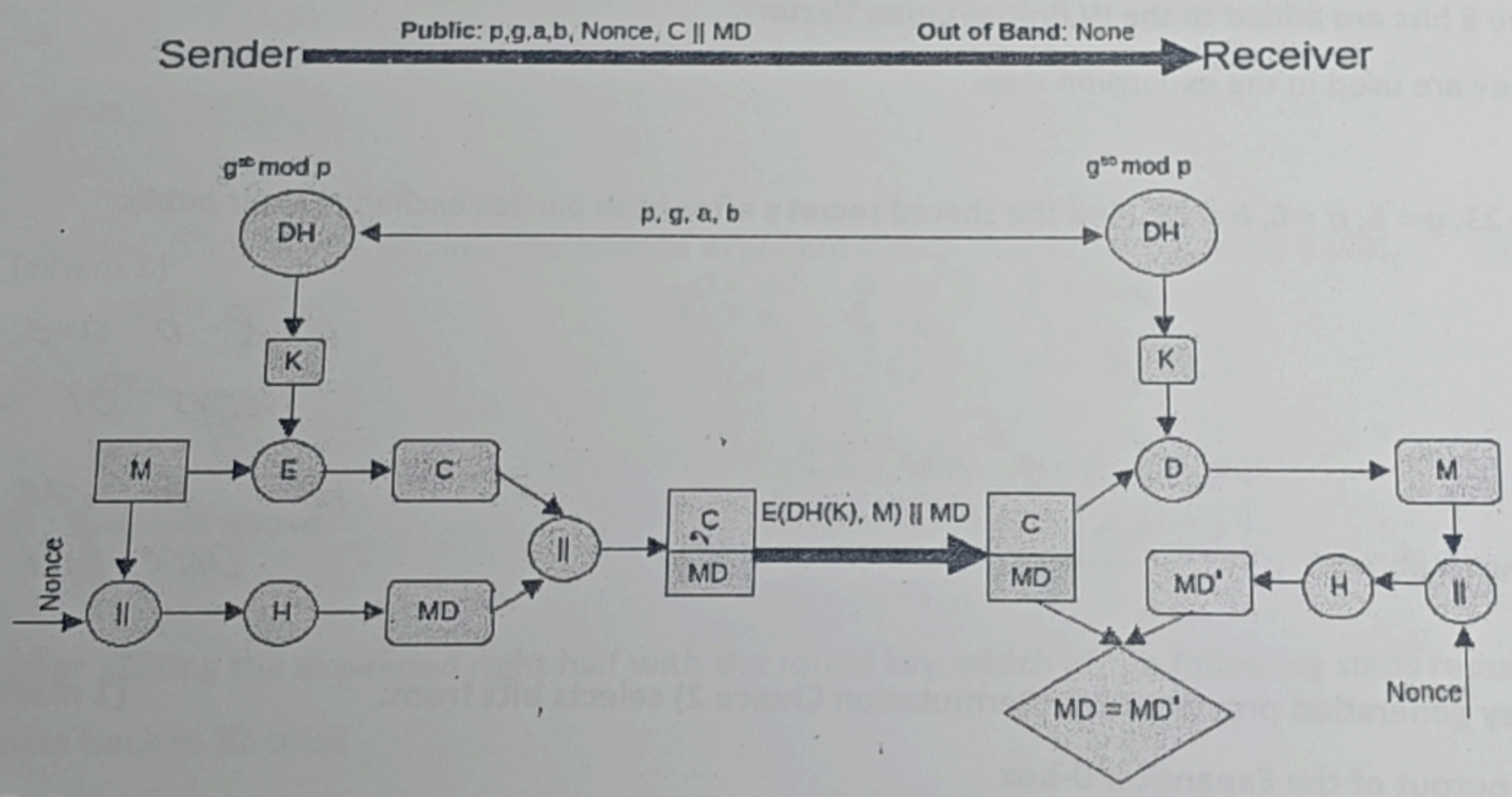
I: Unauthorized modification/insertion/deletion is detectable by crypto- graphic checks.

A: Sender or data source is verified via credentials/keys/signatures

NR: Cryptographic proof of origin/action prevents later denial.

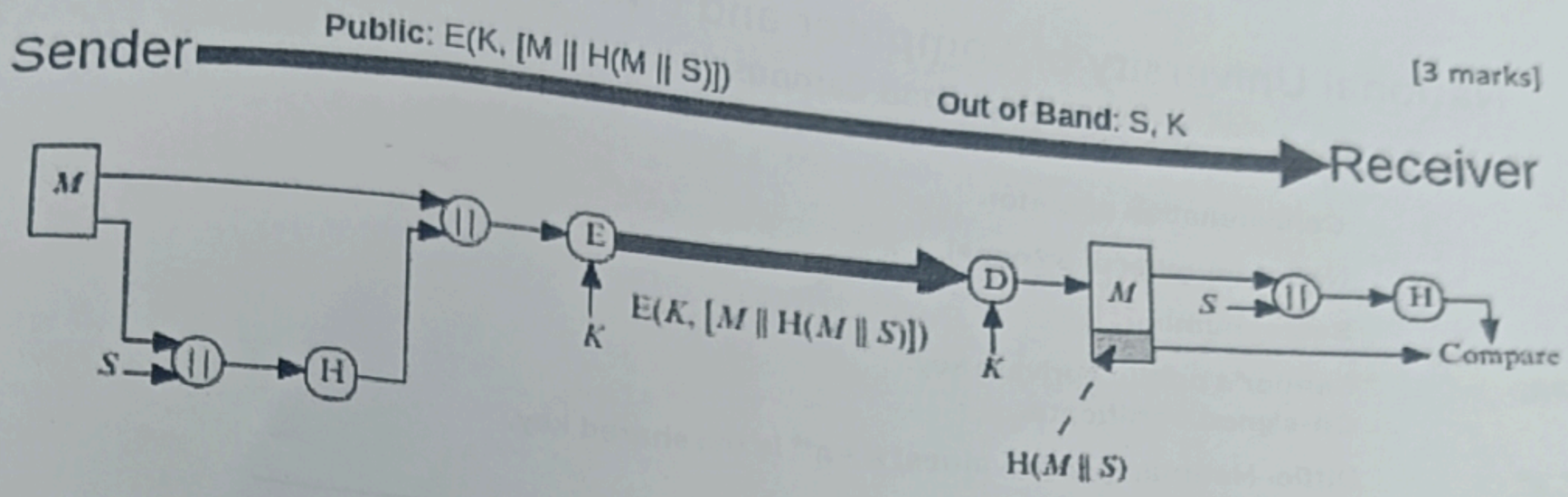
F: Message is recent, i.e., not a replay of a previous valid exchange.

10. **[3 marks]**



a) C, I
b) C, I, F
c) C, I, A
d) C, I, A, NR
e) C, I, A, NR, F
f) None of the Above

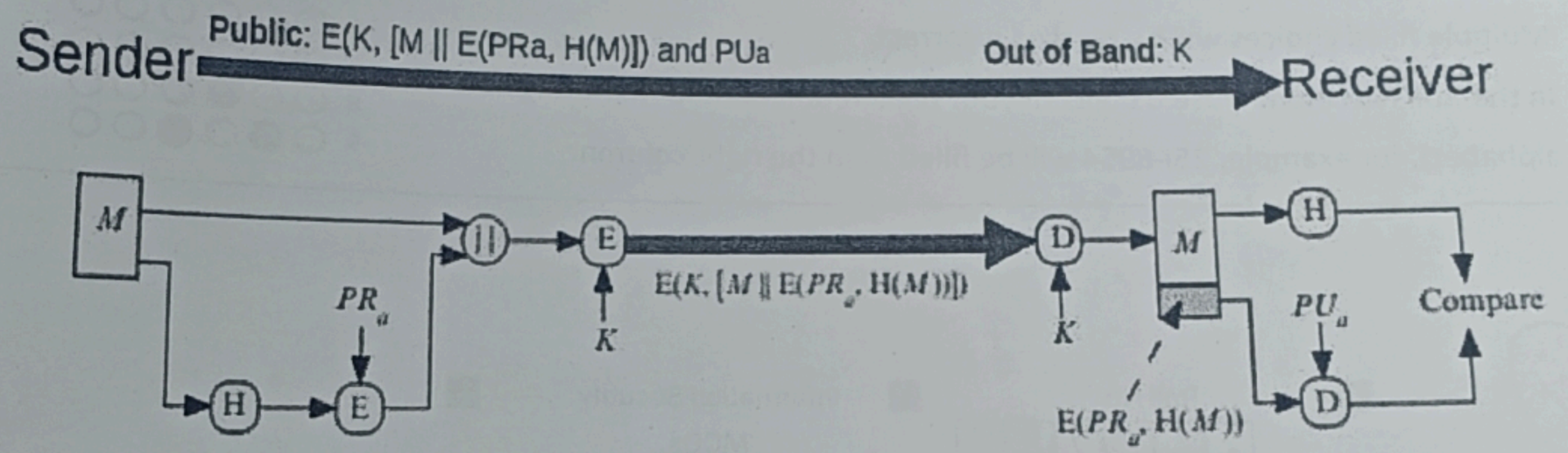
11.



[3 marks]

a) C, I
b) C, I, F
c) C, I, A
d) C, I, A, NR
e) C, I, A, NR, F
f) None of the Above

12.



[3 marks]

a) I, F
b) I, A, F
c) C, I, A
d) C, I, A, NR
e) C, I, A, NR, F
f) None of the Above

Glossary (symbols)

M	Plaintext message.
H	Cryptographic hash.
MD	Message Digest generated by hash function.
E/D	Encrypt / Decrypt primitives.

Extra Work/ Calculations:

d) Third Word = $\begin{bmatrix} B8 \\ 41 \\ 11 \\ F1 \end{bmatrix}$; For 2nd Byte [01 02 03 01]

=> (01 x B8) ⊕ (02 x 41) ⊕ (03 x 11) ⊕ (01 x F1)

Here,

01 x B8 = B8 ;

01 x F1 = F1

but,

02 x 41 => First convert 41_{16} into binary

$41_{16} = 0100\ 0001_2$

∵ MSB = 0, we can simply do left shift by 1

∴ 02 x 41 = $1000\ 0010_2 = 82_{16}$

&, 03 x 11 = (02 x 11) ⊕ (01 x 11)

=> 02 x 11 => $0001\ 0001_2$ ∵ MSB = 0 we can simply do left shift

=> $0010\ 0010_2$

$= 22_{16}$

=> (03 x 11) = (22) ⊕ (11) ∵ 01 x 11 = 11

= 33_{16}

=> (B8) ⊕ (82) ⊕ (33) ⊕ F1 = F8

#	Option	marks
1	c	1
2	A	2
3	b,d	2
4	c	1
5	a,d	2
6	c,d	2
7	a	2
8	a	1
8	d	2
9	b	1
10	f	3
11	c	3
12	c	3