USN | | | | | | | | | | |

Internal Assessment Test 1 – September 2025

Sub:	**Cryptography & Network Security**					Sub Code:	**BCS703**	Branch:	**CSE -AIML**	
Date:	**29/ 9 /25**	Duration:	**90 minutes**	Max Marks:	**50**	Sem/Sec:	**V**			**OBE**

		Answer any FIVE FULL Questions	**MARKS**	**CO**	**RBT**
1	a	Explain the play fair cipher and encrypt the plaintext: SWARAJ IS MY BIRTH RIGHT by using the key "MONARCHY". Use 'X' for blank spaces.	[10]	2	L3
2	a	Discuss the general description of DES encryption algorithm with the aid of diagram.	[10]	3	L2
3	a	Illustrate the RSA algorithm. Find the decryption key 'd' by using n=143 and encryption key e=11.	[10]	1	L3
4	a	What are the requirements for public key cryptosystems? Explain.	[10]	2	L2
5	a	Consider a Diffie-Hellman scheme with a common prime p=11and primitive root **α**=2 (Alpha) (i) Show that 2 is a primitive root of 11 (ii) If user 'A' has public key Y_A=9, What is A's private key X_A? (iii) If user 'B' has public key Y_B=9, What is the shared key K, share with A?	[10]	2	L3
6	a	Apply the Hill Cipher algorithm to encrypt the plaintext "PAYMOREMONEY" by using the key $K = \begin{matrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{matrix}$ show all the calculations.	[10]	3	L3

CI **CCI** **HoD**

1 a Explain the play fair cipher and encrypt the plaintext: SWARAJ IS MY BIRTH RIGHT by using the key "MONARCHY". Use 'X' for blank spaces.

Plaintext: SWARAJ IS MY BIRTH RIGHT
Key: MONARCHY
Rule: Use X for spaces.

Step 1: Construct the 5×5 Playfair matrix

- Key = MONARCHY (remove duplicates).
- Then fill remaining letters of alphabet (I/J considered same).

M O N A R

C H Y B D

E F G I/J K

L P Q S T

U V W X Z

Step 2: Prepare the plaintext

- Replace spaces with X:
  SWARAJXISXMYXBIRTHXRIGHT
- Split into digraphs (pairs). If same letters in a pair, insert X between them.

SW AR AJ XI SX MY XB IR TH XR IG HT

Step 3: Apply Playfair encryption rules

Rules:

1. Same row → take right letter (wrap around if needed).
2. Same column → take letter below (wrap around if needed).
3. Otherwise → take rectangle rule (opposite corners).

Now encrypt each digraph:

1. **SW** → (S row4 col4, W row5 col3) → rectangle → QX
2. **AR** → (A row1 col4, R row1 col5) → same row → RM
3. **AJ** → (A row1 col4, J=I row3 col4) → same col → IS
4. **XI** → (X row5 col4, I row3 col4) → same col → AS
5. **SX** → (S row4 col4, X row5 col4) → same col → AU
6. **MY** → (M row1 col1, Y row2 col3) → rectangle → NC
7. **XB** → (X row5 col4, B row2 col4) → same col → AI
8. **IR** → (I row3 col4, R row1 col5) → rectangle → AK
9. **TH** → (T row4 col5, H row2 col2) → rectangle → PC
10. **XR** → (X row5 col4, R row1 col5) → rectangle → AM
11. **IG** → (I row3 col4, G row3 col3) → same row → FK
12. **HT** → (H row2 col2, T row4 col5) → rectangle → DS

Step 4: Final Ciphertext

Concatenate all:

QX RM IS AS AU NC AI AK PC AM FK DS

Or as one string:

QXRMISASAUNCaIAKPCAMFKDS

✅ **Final Answer:**
Using Playfair cipher with key **MONARCHY**, the ciphertext is:
QXRMISASAU NCAIAKPCAMFKDS

---

2 a Discuss the general description of DES encryption algorithm with the aid of diagram. [10] 3 L2

General Description of DES Encryption Algorithm

The **Data Encryption Standard (DES)** is a **block cipher** developed by IBM and adopted as a standard by NIST in 1977.

- **Block size**: 64 bits
- **Key size**: 64 bits (but only 56 bits are effective, 8 bits used for parity)
- **Rounds**: 16 rounds of encryption (Feistel structure)
- **Output**: 64-bit ciphertext

Working Steps of DES

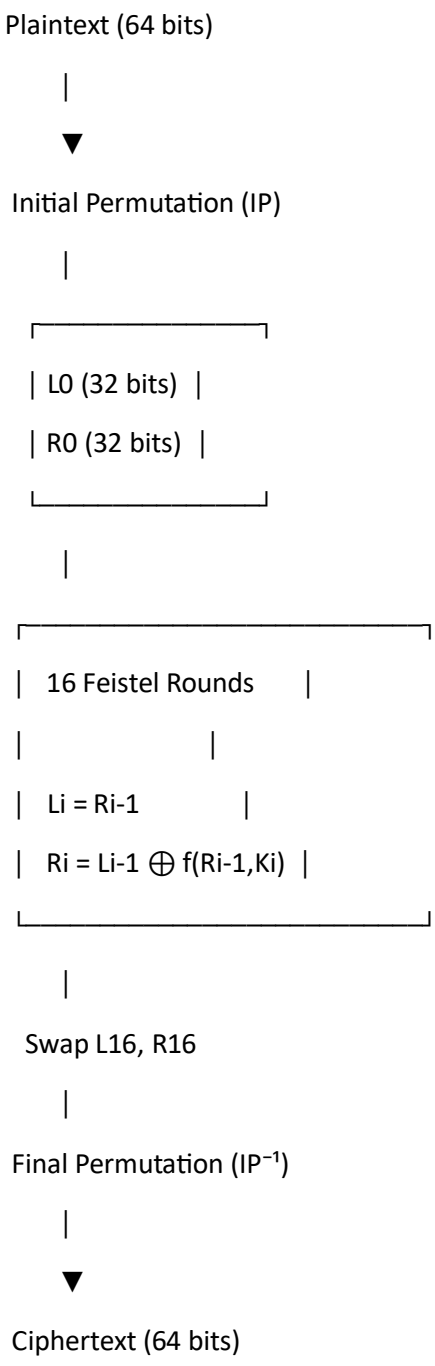
1. **Initial Permutation (IP):**
    - The 64-bit plaintext is permuted according to a fixed table.
    - This shuffles the bits to prepare for processing.
2. **Division into Halves:**
    - After IP, the block is divided into two 32-bit halves: **Left (L0)** and **Right (R0)**.
3. **16 Feistel Rounds:**
    - Each round uses the Feistel structure:
        - Input: (Li-1, Ri-1)
        - Output:
        - Li = Ri-1
        - Ri = Li-1 $\oplus$ f(Ri-1, Ki)
        - Here f is the **round function** and Ki is the subkey for that round.
    - **Round Function f(R, K):**
        - **Expansion (E-box):** Expand 32-bit R to 48 bits.
        - **XOR with Subkey:** Combine with 48-bit Ki.
        - **Substitution (S-box):** Divide into 8 groups of 6 bits → compress into 4 bits each → 32 bits.
        - **Permutation (P-box):** Rearranges 32-bit result.
        - Output is given to XOR with L.
4. **Final Permutation (FP):**
    - After 16 rounds, swap L16 and R16.
    - Apply the **Inverse Initial Permutation (IP^{-1})** to get the 64-bit ciphertext.

Key Generation in DES

- Input key: 64 bits (only 56 used, 8 discarded as parity).

- Using permutation and shifts, generate **16 subkeys**, each of 48 bits, one for each round.

Diagram of DES (Textual form)



---

3 a Illustrate the RSA algorithm. Find the decryption key 'd' by using n=143 and encryption key e=11.

RSA — brief illustration and calculation of ddd

1. Quick outline of RSA (steps)

1. Choose two distinct primes ppp and qqq.
2. Compute n=pqn=pqn=pq. nnn is the modulus.
3. Compute Euler's totient ϕ(n)=(p−1)(q−1)\varphi(n)=(p-1)(q-1)ϕ(n)=(p−1)(q−1).
4. Choose public exponent eee such that 1<e<ϕ(n)1<e<\varphi(n)1<e<ϕ(n) and gcd(e,ϕ(n))=1\gcd(e,\varphi(n))=1gcd(e,ϕ(n))=1.

5. Find private exponent ddd satisfying e·d≡1(modϕ(n))e\cdot d \equiv 1 \pmod{\varphi(n)}e·d≡1(modϕ(n)) (i.e. ddd is the modular inverse of eee modulo ϕ(n)\varphi(n)ϕ(n)).
6. Public key = (n,e)(n,e)(n,e). Private key = ddd.
7. Encryption for message mmm (with 0≤m<n0\le m<n0≤m<n): c≡me(modn)c\equiv m^{e}\pmod{n}c≡me(modn).
8. Decryption: m≡cd(modn)m\equiv c^{d}\pmod{n}m≡cd(modn).

---

2. Given data

- n=143n=143n=143
- e=11e=11e=11

Factor nnn: 143=11×13143=11\times 13143=11×13. So choose p=11, q=13p=11,\; q=13p=11,q=13.

Compute ϕ(n)=(p−1)(q−1)=10×12=120\varphi(n)=(p-1)(q-1)=10\times12=120ϕ(n)=(p−1)(q−1)=10×12=120.

We must find ddd such that

11·d≡1(mod120).11\cdot d \equiv 1 \pmod{120}.11·d≡1(mod120).

---

3. Compute ddd (extended Euclidean steps)

We need the inverse of 111111 modulo 120120120.

Do Euclid's algorithm:

- 120=11×10+10120 = 11\times10 + 10120=11×10+10
- 11=10×1+111 = 10\times1 + 111=10×1+1
- 10=1×10+010 = 1\times10 + 010=1×10+0

Back-substitute to express 1 as combination of 11 and 120:

- 1=11−10×11 = 11 - 10\times11=11−10×1
- but 10=120−11×1010 = 120 - 11\times1010=120−11×10

So

1=11−(120−11×10)=11−120+11×10=11×11−120×1.1 = 11 - (120 - 11\times10) = 11 - 120 + 11\times10 = 11\times11 - 120\times1.1=11−(120−11×10)=11−120+11×10=11×11−120×1.

Thus 11×11≡1(mod120)11\times11 \equiv 1 \pmod{120}11×11≡1(mod120). Therefore

d≡11(mod120).d \equiv 11 \pmod{120}.d≡11(mod120).

We can take the smallest positive d=11d = 11d=11.

---

4. Verification

11·11=121≡1(mod120)11\cdot 11 = 121 \equiv 1 \pmod{120}11·11=121≡1(mod120). ✅

So the private (decryption) exponent is **d=11d = 11d=11**.
(Interesting observation: here e=de=de=d — the public exponent equals the private exponent modulo ϕ(n)\varphi(n)ϕ(n).)

---

4 a What are the requirements for public key cryptosystems? Explain.

Requirements for Public Key Cryptosystems

A **public key cryptosystem** is an asymmetric system where each user has a **pair of keys**:

- **Public key** (known to everyone)
- **Private key** (kept secret)

For such a system to be secure and practically usable, the following requirements must be satisfied:

---

1. Computational Feasibility

- It must be **easy (efficient)** to generate a key pair (e,d)(e,d)(e,d) and to encrypt/decrypt a message using the respective keys.
- Example: RSA encryption and decryption are efficient with modular exponentiation.

---

2. One-way Function Property

- Given the public key eee and ciphertext CCC, it should be computationally **infeasible** to determine the plaintext MMM without the private key ddd.
- Ensures security even if public key is widely distributed.

---

3. Trapdoor Function Property

- The system should be based on a **mathematical function** that is easy to compute in one direction but hard to invert **unless special secret information (trapdoor)** is known.
- Example: Multiplying two large primes is easy, but factoring their product (RSA modulus) is hard.

---

4. Key Pair Relationship

- A message encrypted with the **public key** can only be decrypted with the corresponding **private key**, and vice versa.
- This ensures both **confidentiality** (encryption) and **authentication** (digital signatures).

---

5. Resistance to Attacks

- It should be computationally infeasible to derive the **private key** from the **public key**.
- The system must withstand known cryptanalytic attacks (e.g., brute force, factoring, discrete logarithm).

---

6. Scalability

- Each participant should only need to keep a single key pair (public + private), while the public keys can be freely distributed.
- This removes the need for n(n−1)/2n(n-1)/2n(n−1)/2 secret keys as in symmetric cryptography.

---

5 a Consider a Diffie-Hellman scheme with a common prime p=11and primitive root α=2 (Alpha) (i) Show that 2 is a primitive root of 11 (ii) If user 'A' has public key YA=9, What is A's private key XA? (iii) If user 'B' has public key YB=9, What is the shared key K, share with A? [10] 2 L3

(i) Show 2 is a primitive root of 11

Compute powers of 2 modulo 11:

$$
\begin{aligned}
2^1 &\equiv 2 \pmod{11} \\
2^2 &\equiv 4 \pmod{11} \\
2^3 &\equiv 8 \pmod{11} \\
2^4 &\equiv 16 \equiv 5 \pmod{11} \\
2^5 &\equiv 2^4 \cdot 2 \equiv 5 \cdot 2 = 10 \pmod{11} \\
2^6 &\equiv 10 \cdot 2 = 20 \equiv 9 \pmod{11} \\
2^7 &\equiv 9 \cdot 2 = 18 \equiv 7 \pmod{11} \\
2^8 &\equiv 7 \cdot 2 = 14 \equiv 3 \pmod{11} \\
2^9 &\equiv 3 \cdot 2 = 6 \pmod{11} \\
2^{10} &\equiv 6 \cdot 2 = 12 \equiv 1 \pmod{11}.
\end{aligned}
$$

The powers $2^1, \ldots, 2^{10}$ produce the residues $\{2, 4, 8, 5, 10, 9, 7, 3, 6, 1\}$ — i.e. all nonzero residues modulo 11. So the order of 2 modulo 11 is 10 (which equals $p - 1$), therefore **2 is a primitive root of 11.**

(ii) Find A's private key X_A given public key $Y_A = 9$

Public key $Y_A \equiv \alpha^{X_A} \pmod{p}$. We need X_A with $2^{X_A} \equiv 9 \pmod{11}$.

From the table above $2^6 \equiv 9 \pmod{11}$. Thus $X_A = 6$ (smallest positive exponent giving 9).

(iii) If $Y_B = 9$, what is the shared key K between A and B?

Diffie–Hellman shared key $K \equiv Y_B^{X_A} \pmod{p}$. With $Y_B = 9$ and $X_A = 6$:

$$K \equiv 9^6 \pmod{11}.$$

Compute $9^2 \equiv 81 \equiv 4$, so $9^6 = (9^2)^3 \equiv 4^3 = 64 \equiv 64 - 5 \cdot 11 = 64 - 55 = 9 \pmod{11}$.
(Also note $2^{36} \equiv 2^{36 \bmod 10} = 2^6 \equiv 9$.)

So the shared key is $K = 9$.

Final answers

(i) 2 is a primitive root of 11.
(ii) $X_A = 6$.
(iii) Shared key $K = 9$.

6.a Apply the Hill Cipher algorithm to encrypt the plaintext "PAYMOREMONEY" by using the key K = 17 17 5 ,21 18 21 ,2 2 19 show all the calculations.

$$K = \begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix}$$

and the plaintext is still "**PAYMOREMONEY**". Let's carefully redo the **Hill Cipher encryption** step by step.

Step 1: Convert plaintext to numbers

A=0, B=1, ..., Z=25

```mathematica
P → 15
A → 0
Y → 24
M → 12
O → 14
R → 17
E → 4
M → 12
O → 14
N → 13
E → 4
Y → 24
```

Numbers:

$$[15, 0, 24, 12, 14, 17, 4, 12, 14, 13, 4, 24]$$

Split into **3×1 blocks**:

$$P_1 = \begin{bmatrix} 15 \\ 0 \\ 24 \end{bmatrix},\ P_2 = \begin{bmatrix} 12 \\ 14 \\ 17 \end{bmatrix},\ P_3 = \begin{bmatrix} 4 \\ 12 \\ 14 \end{bmatrix},\ P_4 = \begin{bmatrix} 13 \\ 4 \\ 24 \end{bmatrix}$$

Step 2: Encrypt using Hill Cipher formula

$$C = K \cdot P \mod 26$$

Block 1: $P_1 = \begin{bmatrix} 15 \\ 0 \\ 24 \end{bmatrix}$

$$C_1 = \begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix} \begin{bmatrix} 15 \\ 0 \\ 24 \end{bmatrix} \mod 26$$

Compute each element:

1. Row 1: $17 * 15 + 17 * 0 + 5 * 24 = 255 + 0 + 120 = 375 \mod 26$
   $26 * 14 = 364$, remainder $375 - 364 = 11 \rightarrow 11 \rightarrow$ L
2. Row 2: $21 * 15 + 18 * 0 + 21 * 24 = 315 + 0 + 504 = 819 \mod 26$
   $26 * 31 = 806$, remainder $819 - 806 = 13 \rightarrow 13 \rightarrow$ N
3. Row 3: $2 * 15 + 2 * 0 + 19 * 24 = 30 + 0 + 456 = 486 \mod 26$
   $26 * 18 = 468$, remainder $486 - 468 = 18 \rightarrow 18 \rightarrow$ S

Block 1 ciphertext: LNS

Block 2: $P_2 = \begin{bmatrix} 12 \\ 14 \\ 17 \end{bmatrix}$

1. Row 1: $17 * 12 + 17 * 14 + 5 * 17 = 204 + 238 + 85 = 527$
   $26 * 20 = 520$, remainder 7 → 7 → **H**
2. Row 2: $21 * 12 + 18 * 14 + 21 * 17 = 252 + 252 + 357 = 861$
   $26 * 33 = 858$, remainder 3 → 3 → **D**
3. Row 3: $2 * 12 + 2 * 14 + 19 * 17 = 24 + 28 + 323 = 375$
   $26 * 14 = 364$, remainder 11 → 11 → **L**

Block 2 ciphertext: HDL

Block 3: $P_3 = \begin{bmatrix} 4 \\ 12 \\ 14 \end{bmatrix}$

1. Row 1: $17 * 4 + 17 * 12 + 5 * 14 = 68 + 204 + 70 = 342$
   $26 * 13 = 338$, remainder 4 → 4 → **E**
2. Row 2: $21 * 4 + 18 * 12 + 21 * 14 = 84 + 216 + 294 = 594$
   $26 * 22 = 572$, remainder 22 → 22 → **W**
3. Row 3: $2 * 4 + 2 * 12 + 19 * 14 = 8 + 24 + 266 = 298$
   $26 * 11 = 286$, remainder 12 → 12 → **M**

Block 3 ciphertext: EWM

Block 4: $P_4 = \begin{bmatrix} 13 \\ 4 \\ 24 \end{bmatrix}$

1. Row 1: $17 * 13 + 17 * 4 + 5 * 24 = 221 + 68 + 120 = 409$
   $26 * 15 = 390$, remainder 19 → 19 → **T**
2. Row 2: $21 * 13 + 18 * 4 + 21 * 24 = 273 + 72 + 504 = 849$
   $26 * 32 = 832$, remainder 17 → 17 → **R**
3. Row 3: $2 * 13 + 2 * 4 + 19 * 24 = 26 + 8 + 456 = 490$
   $26 * 18 = 468$, remainder 22 → 22 → **W**

Block 4 ciphertext: TRW

Step 3: Combine all blocks

$$\text{Ciphertext} = LNSHDLEW\,MTRW$$

✅ Final Answer

Plaintext: `PAYMOREMONEY`

Ciphertext (Hill Cipher 3×3):