Unit 1: Overview & Classical Encryption

Q: What is the NIST definition of Computer Security?

A: "The protection afforded to an automated information system in order to attain the applicable objectives of preserving the **integrity, availability, and confidentiality** of information system resources (includes hardware, software, firmware, information/data, and telecommunications)."

Q: What are the three key objectives of the CIA Triad? A:

- **Confidentiality:** Preserving authorized restrictions on information access and disclosure. A loss of confidentiality is the unauthorized disclosure of information.
- **Integrity:** Guarding against improper information modification or destruction. A loss of integrity is the unauthorized modification or destruction of information.
- **Availability:** Ensuring timely and reliable access to and use of information. A loss of availability is the disruption of access to or use of information.

Q: What is the difference between a security attack, mechanism, and service? A:

- **Security Attack:** Any action that compromises the security of information owned by an organization.
- **Security Mechanism:** A process (or device) designed to detect, prevent, or recover from a security attack.
- **Security Service:** A communication service that enhances the security of data processing systems and information transfers. It is intended to counter security attacks and uses one or more security mechanisms.

Q: What is the difference between passive and active security attacks? A:

- **Passive Attacks:** Involve eavesdropping on or monitoring transmissions. The goal is to obtain information without modifying it. The two types are **Release of message contents** and **Traffic analysis**.
- **Active Attacks:** Involve some modification of the data stream or the creation of a false stream.

Q: (From Test Paper) Explain the Active Security attacks attack types in detail.

A: Active attacks involve modifying the data stream or creating a false one. The four main categories are:

1. **Masquerade (Impersonation):** This takes place when one entity pretends to be a different entity. An example is logging in using stolen credentials.
2. **Replay:** This involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect. An example is reusing a payment request message to withdraw money a second time.
3. **Modification of messages:** This means that some portion of a legitimate message is altered, or messages are delayed or reordered, to produce an unauthorized effect. An example is altering a message from "Allow John Smith to read..." to "Allow Fred Brown to read...".
4. **Denial of Service (DoS):** This prevents or inhibits the normal use or management of communications facilities. It can be done by disabling a network or overloading it with messages to degrade performance. An example is flooding a server with requests so real users cannot log in.

Q: What are the two requirements for the secure use of conventional (symmetric) encryption? A:

1. A **strong encryption algorithm** is needed. The opponent should be unable to decrypt the ciphertext or discover the key, even with access to multiple ciphertexts and their corresponding plaintexts.
2. The sender and receiver must **obtain copies of the secret key in a secure fashion** and must keep the key secure.

Q: (From Test Paper) Explain Caesar cipher and encrypt the text "Attack At Seven". A:

- **Explanation:** The Caesar cipher is a substitution technique where each letter of the alphabet is replaced by the letter standing **three places further down** the alphabet.
- The general algorithm is $C=E(k,p)=(p+k) \mod 26$, where p is the numerical value of the plaintext letter, k is the shift (key), and C is the numerical value of the ciphertext letter. For the standard Caesar cipher, the key k is 3.

- The decryption algorithm is p=D(k,C)=(C−k)mod26.
- **Encryption:**
    1. **Plaintext:** "Attack At Seven"
    2. **Convert to single case** (following the slide example `meet me...` → `PHHW PH...`): "ATTACK AT SEVEN"
    3. **Apply k=3 shift:**
        - A (0) + 3 = **D** (3)
        - T (19) + 3 = **W** (22)
        - T (19) + 3 = **W** (22)
        - A (0) + 3 = **D** (3)
        - C (2) + 3 = **F** (5)
        - K (10) + 3 = **N** (13)
        - (space) → (space)
        - A (0) + 3 = **D** (3)
        - T (19) + 3 = **W** (22)
        - (space) → (space)
        - S (18) + 3 = **V** (21)
        - E (4) + 3 = **H** (7)
        - V (21) + 3 = **Y** (24)
        - E (4) + 3 = **H** (7)
        - N (13) + 3 = **Q** (16)
    4. **Ciphertext: "DWWDFN DW VHYHQ"**

Q: Explain the encryption rules for the Playfair Cipher.

A: The Playfair cipher uses a 5x5 matrix built from a keyword. It encrypts plaintext by treating pairs of letters (digrams) as single units.

1. **Filler Letter:** Repeating plaintext letters in the same pair are separated with a filler letter, such as 'x'.
2. **Same Row:** If two plaintext letters fall in the same row, each is replaced by the letter to its **right**, with the first element of the row circularly following the last.
3. **Same Column:** If two plaintext letters fall in the same column, each is replaced by the letter **beneath** it, with the top element of the column circularly following the last.
4. **Rectangle:** Otherwise, each plaintext letter is replaced by the letter that lies in its **own row and the column occupied by the other** plaintext letter.

Q: How does the Vigenere Cipher work?

A: The Vigenere cipher is a **polyalphabetic substitution** cipher, meaning it uses multiple substitution alphabets.

1. It uses a **keyword**.
2. This keyword is repeated in a circular manner until it matches the length of the plaintext.
3. Each letter of the plaintext is then encrypted using the corresponding letter of the repeated key by referencing a **Vigenère square** (or table).
4. Mathematically, the encryption is Ei=(Pi+Ki)mod26, where Pi is the plaintext letter and Ki is the corresponding keyword letter.

Unit 2: Block Ciphers, DES, & AES

Q: What is the difference between a Block Cipher and a Stream Cipher? A:

- A **Stream Cipher** encrypts a digital data stream one bit or one byte at a time.
- A **Block Cipher** takes a block of plaintext (e.g., 64 or 128 bits) and treats it as a whole, producing a ciphertext block of equal length.

Q: Explain the concepts of Diffusion and Confusion. A:

- **Diffusion:** This property dissipates the statistical structure of the plaintext across the ciphertext. It is achieved by having each plaintext digit affect the value of many ciphertext digits. This is generally done using **permutation (or transposition)**.
- **Confusion:** This property aims to make the relationship between the encryption key and the ciphertext as complex as possible. This is achieved using **substitution**.

Q: (From Test Paper) With a neat diagram explain Feistel Encryption and Decryption algorithm. A:

- **Feistel Encryption:** The Feistel cipher is a design structure used to build block ciphers like DES.
    1. The input plaintext block is split into two equal halves, a left half (L0) and a right half (R0) .
    2. The cipher then goes through multiple rounds (e.g., 16 rounds).

3. In each round i, the following operations occur:
    - The left half of the next round is set to be the right half of the current round: $L_i = R_{i-1}$.
    - The right half of the next round is calculated by taking the left half of the current round and XORing it with the output of a round function F: $R_i = L_{i-1} \oplus F(R_{i-1}, K_i)$.
4. The function F is the round function (which provides confusion), and Ki is the subkey for that round.
5. After the final round, a final swap of the left and right halves is performed to produce the ciphertext.

- **Feistel Decryption:** The decryption process uses the **exact same algorithm** as encryption. The only difference is that the **round subkeys (K1,K2,...K16) are applied in the reverse order** (e.g., K16 is used in the first decryption round, K15 in the second, and so on).

Q: (From Test Paper) Illustrate Avalanche Effect with example. A:

- **Illustration:** The **Avalanche Effect** is a desirable property for any encryption algorithm. It means that a small change in the input (either a single bit of the **plaintext** or a single bit of the **key**) should produce a significant change in the output **ciphertext**.
- **Example:** In DES, this effect is strong. A 1-bit change in the plaintext (e.g., changing `0000...` to `1000...`) results in, on average, 34 bits of the 64-bit ciphertext being different. Similarly, changing one bit in the key while keeping the plaintext the same also results in a completely different ciphertext. This prevents attackers from finding patterns or deducing the key by making small changes to the plaintext.

Q: What are the four transformation functions used in each round of AES?

A: AES does not use a Feistel structure; instead, it processes the entire data block in each round. Each round (except the last) consists of four stages:

1. **Substitute Bytes:** A non-linear byte-by-byte substitution using a predefined lookup table called an **S-box**.
2. **ShiftRows:** A simple permutation where the bytes in the last three rows of the 4x4 state matrix are cyclically shifted to the left by different offsets.

3. **MixColumns:** A transformation that operates on each column of the state individually, combining the four bytes in each column using arithmetic in GF(28).
4. **AddRoundKey:** The state is bitwise XORed with the round key for that round.

Q: (From Test Paper) Illustrate the key expansion function of AES algorithm. A: The AES **Key Expansion** function generates a schedule of round keys from the initial cipher key. The number of round keys needed depends on the number of rounds (e.g., 10 rounds for a 128-bit key).

The expansion for a 128-bit key (which is 4 words) works as follows:

- The first four words of the expanded key (w[0] to w[3]) are the original cipher key.
- Every subsequent word w[i] is generated by XORing the previous word w[i−1] with the word from four positions back w[i−4].
- **Special Step:** If i is a multiple of 4, a special function g is applied to w[i−1] *before* the XOR. This g function consists of:
    1. **RotWord:** A one-byte circular left shift of the 4-byte word.
    2. **SubWord:** Each of the four bytes is passed through the AES S-box (the same one used in Substitute Bytes).
    3. **Rcon XOR:** The result is XORed with a **Round Constant (Rcon)**, which is a different value for each round.

This process ensures that each round key is unique and non-linearly related to the original cipher key.

Unit 3: Public-Key Cryptography

Q: (From Test Paper) Explain the requirements of public key cryptography.

A: This topic, "Requirements for public-key cryptosystems," is listed as part of Unit III in the syllabus. However, the provided documents (1.pdf, 2.pdf) do not contain the slides that explain these requirements in detail.

🏛️ Unit 1: Solutions

1. Caesar Cipher (Decryption)

- **Question:** Decrypt the ciphertext: **"VHFXUHB FRPSXWLQJ"** (using $k=3$).

- **Solution:** Decryption involves shifting each letter **left by 3** (or $p = (C - 3) \mod 26$).
    - V $\rightarrow$ S
    - H $\rightarrow$ E
    - F $\rightarrow$ C
    - X $\rightarrow$ U
    - U $\rightarrow$ R
    - H $\rightarrow$ E
    - B $\rightarrow$ Y (B is 1, $1-3 = -2 \rightarrow 24$, which is Y)
    - (space)
    - F $\rightarrow$ C
    - R $\rightarrow$ O
    - P $\rightarrow$ M
    - S $\rightarrow$ P
    - X $\rightarrow$ U
    - W $\rightarrow$ T
    - L $\rightarrow$ I
    - Q $\rightarrow$ N
    - J $\rightarrow$ G
- **Plaintext: "SECURE COMPUTING"**

---

2. Mono-alphabetic Cipher (Conceptual)

- **Question:** Ciphertext 'K' is most frequent, and 'QVK' is the most common trigram. Plaintext 'e' is most frequent, and 'the' is the most common trigram. What is your hypothesis?
- **Solution:** This is a **frequency analysis** attack[1]. By matching the statistics of the ciphertext to the known statistics of the English language, you can form a hypothesis.
    - **Hypothesis:**
        - Ciphertext 'K' $\rightarrow$ Plaintext 'e' (Matching the single-letter frequency)

        - Ciphertext 'Q' $\rightarrow$ Plaintext 't' (From matching 'QVK' to 'the')
        - Ciphertext 'V' $\rightarrow$ Plaintext 'h' (From matching 'QVK' to 'the')

---

3. Playfair Cipher (Encryption)

- **Question:** Using the keyword **"SECURITY"** (I/J combined), encrypt **"MEET AT THE WEST WALL"**.
- **Solution:**
    - Step 1: Create the 5x5 Matrix. (Note: I is in the keyword, so it takes the spot, and J is treated as I).
S	E	C	U	R
I	T	Y	A	B
D	F	G	H	K
L	M	N	O	P
Q	V	W	X	Z
    - **Step 2: Process the Plaintext.** (Remove spaces, split into pairs, add filler 'X' for repeating letters, and pad with 'Z' at the end if needed).
        - MEETATTHEWESTWALL
        - ME ET AT TH EW ES TW AL LX (from WALL $\rightarrow$ WA LL $\rightarrow$ WA LX L...)
        - ME ET AT TH EW ES TW AL LX LZ (Padded final 'L' with 'Z')
    - **Step 3: Encrypt the Pairs.** [2]
        - ME: Rectangle (Row 4, Row 1) $\rightarrow$ **LF**
        - ET: Same Row (Row 1, Row 2) $\rightarrow$ **CY**
        - AT: Same Column (Col 4, Col 2) $\rightarrow$ **TY**
        - TH: Rectangle (Row 2, Row 3) $\rightarrow$ **YG**
        - EW: Rectangle (Row 1, Row 5) $\rightarrow$ **CV**
        - ES: Same Row (Row 1, Row 1) $\rightarrow$ **CS**

        - TW: Rectangle (Row 2, Row 5) $\rightarrow$ **YV**
        - AL: Rectangle (Row 2, Row 4) $\rightarrow$ **IM**
        - LX: Rectangle (Row 4, Row 5) $\rightarrow$ **NQ**
        - LZ: Rectangle (Row 4, Row 5) $\rightarrow$ **PV**
- **Ciphertext: "LFCYTY YGCVCS YVIMNQ PV"**

🖥️ Unit 2: Solutions

1. S-DES (Key Generation)

- **Question:** Given 10-bit key **1110001110**, find K_1 (using P10: 3-5-2-7-4-10-1-9-8-6 and P8: 6-3-7-4-8-5-10-9).
- **Solution:**
    - **Part A (P10):** Apply P10 to the key.
        - **Key:** 1 1 1 0 0 0 1 1 1 0 (Positions 1-10)
        - **P10:** 1 0 1 1 0 0 1 1 1 0 (Taking pos 3, 5, 2, 7, 4, 10, 1, 9, 8, 6) [3]
    - **Part B (LS-1):** Split the P10 result into two 5-bit halves and perform a 1-bit circular left shift on each.
        - **Split:** 10110 and 01110
        - **LS-1:** 01101 and 11100 [4]
    - **Part C (P8 $\rightarrow$ K_1):** Apply P8 to the 10-bit string from Part B.
        - **Input:** 0 1 1 0 1 1 1 1 0 0 (Positions 1-10)
        - **P8:** 1 1 1 0 1 0 0 1 (Taking pos 6, 3, 7, 4, 8, 5, 10, 9) [5]
- **Key 1 (K_1): 11101001** [6]

---

2. Feistel Cipher (Conceptual)

- **Question:** For a 64-bit plaintext block and 16-round Feistel cipher:
    - A. How many bits are in L_0 and R_0?
    - B. In round 5, what is the formula to calculate R_5?

    - C. After 16 rounds, what is the block *before* the final swap?
- **Solution:**
    - **A:** The block is split into two equal halves. $64 / 2 = $ **32 bits** each [7].
    - **B:** The right half is the XOR of the previous left half and the round function: **$R_5 = L_4 \oplus F(R_4, K_5)$**[8].
    - **C:** The output of the 16th round is **$L_{16} || R_{16}$** (where $||$ means concatenation). The final swap (which is part of the algorithm) would make the ciphertext $R_{16} || [cite_start]L_{16}$ [9].

---

3. AES (Conceptual)

- **Question:**
    - A. What transformation step provides **substitution**?
    - B. What transformation step provides **diffusion** by shifting rows?
    - C. What transformation step provides **diffusion** by mixing data within columns?
- **Solution:**
    - **A: Substitute Bytes** (or SubBytes), which uses the S-box[10101010].
    - **B: ShiftRows**[11111111].
    - **C: MixColumns**[12121212].

🔑 Unit 3: Solutions

1. RSA Key Generation

- **Question:** Given $p = 11$ and $q = 13$:
    - A. Calculate n and $\phi(n)$.

    - B. Is $e = 7$ a valid public exponent?
    - C. Calculate the private exponent d.
- **Solution:**
    - **A:**
        - $n = p \times q = 11 \times 13 = $ **143**.
        - $\phi(n) = (p-1) \times (q-1) = (10) \times (12) = $ **120**.
    - **B: Yes, $e = 7$ is valid.** The requirement is that e must be co-prime to $\phi(n)$ (i.e., $gcd(e, \phi(n)) = 1$). Since $\phi(n) = 120$ (which has factors 2, 3, 5) and $e = 7$ is a prime number not in that list, $gcd(7, 120) = 1$.
    - **C:** We must find d such that $d \times e \equiv 1 \mod \phi(n)$, or $d \times 7 \equiv 1 \mod 120$.
        - Using the Extended Euclidean Algorithm:
        - $120 = 17 \times 7 + 1$
        - Rearrange to solve for 1: $1 = 120 - (17 \times 7)$
        - Taking this $\mod 120$, we get $1 \equiv -17 \times 7 \mod 120$.
        - So, $d \equiv -17 \mod 120$.
        - To find the positive value: $d = 120 - 17 = $ **103**.
        - *(Check: $7 \times 103 = 721$. $721 / 120 = 6.008...$. $6 \times 120 = 720$. $721 - 720 = 1$. It's correct.)*

---

2. RSA Encryption/Decryption

- **Question:** Using $PU = \{7, 143\}$, encrypt $M = 10$. Then, using the d you found, decrypt the result.
- **Solution:**
    - **Encryption:**
        - $C = M^e \mod n = 10^7 \mod 143$
        - $10^1 = 10 \mod 143$
        - $10^2 = 100 \mod 143$
        - $10^4 = 100^2 = 10000 \mod 143$. ($10000 / 143 = 69.9...$; $69 \times 143 = 9867$; $10000 - 9867 = 133$). So, $10^4 \equiv 133 \equiv -10 \mod 143$.

        - $10^7 = 10^4 \times 10^2 \times 10^1 \mod 143$
        - $C = (133 \times 100 \times 10) \mod 143$
        - $C = (13300 \times 10) \mod 143$. ($13300 / 143 = 93.00...$; $93 \times 143 = 13299$; $13300 - 13299 = 1$). So, $13300 \equiv 1$.
        - $C = (1 \times 10) \mod 143 = $ **10**.
    - **Decryption:** (Using $PR = \{103, 143\}$)
        - $M = C^d \mod n = 10^{103} \mod 143$
        - 103 (in binary) $= 64 + 32 + 4 + 2 + 1$.
        - $10^1 = 10$
        - $10^2 = 100$
        - $10^4 \equiv 133$
        - $10^8 = (10^4)^2 \equiv 133^2 = 17689 \mod 143$. ($17689 / 143 = 123.6...$; $123 \times 143 = 17589$; $17689 - 17589 = 100$). So, $10^8 \equiv 100$.
        - $10^{16} = (10^8)^2 \equiv 100^2 \equiv 133$.
        - $10^{32} = (10^{16})^2 \equiv 133^2 \equiv 100$.
        - $10^{64} = (10^{32})^2 \equiv 100^2 \equiv 133$.
        - Now multiply the parts for $10^{103} = 10^{64} \times 10^{32} \times 10^4 \times 10^2 \times 10^1$:
        - $M = (133 \times 100 \times 133 \times 100 \times 10) \mod 143$
        - We already know $133 \times 100 \equiv 1 \mod 143$.
        - $M = (1 \times 1 \times 10) \mod 143 = $ **10**.
- **Result:** The original plaintext **10** is recovered.

---

3. Diffie-Hellman Key Exchange

- **Question:** $p = 23$, $g = 5$. Alice's secret $a = 4$. Bob's secret $b = 3$.
    - A. What is Alice's public key A?
    - B. What is Bob's public key B?
    - C. What is the shared secret S?
- **Solution:**

    - **A. Alice's Public Key (A):**
        - $A = g^a \mod p = 5^4 \mod 23$
        - $5^2 = 25 \equiv 2 \mod 23$
        - $5^4 = (5^2)^2 \equiv 2^2 \mod 23 = $ **4**.
        - Alice sends **$A = 4$** to Bob.
    - **B. Bob's Public Key (B):**
        - $B = g^b \mod p = 5^3 \mod 23$
        - $5^2 = 25 \equiv 2 \mod 23$
        - $5^3 = 5^2 \times 5 \equiv 2 \times 5 \mod 23 = $ **10**.
        - Bob sends **$B = 10$** to Alice.
    - **C. Shared Secret (S):**
        - **Alice computes:** $S = B^a \mod p = 10^4 \mod 23$
        - $10^2 = 100 \equiv (4 \times 23 + 8) \equiv 8 \mod 23$
        - $10^4 = (10^2)^2 \equiv 8^2 = 64 \mod 23$. ($64 = 2 \times 23 + 18$).
        - $S \equiv $ **18**.
        - **Bob computes:** $S = A^b \mod p = 4^3 \mod 23$
        - $4^2 = 16 \mod 23$
        - $4^3 = 16 \times 4 = 64 \mod 23 \equiv $ **18**.
- **Result:** Both parties successfully compute the same shared secret, **$S = 18$**.

Unit 1: Overview & Classical Encryption

Q: What is the NIST definition of Computer Security?

A: "The protection afforded to an automated information system in order to attain the applicable objectives of preserving the **integrity, availability, and confidentiality** of information system resources (includes hardware, software, firmware, information/data, and telecommunications)."

Q: What are the three key objectives of the CIA Triad?

A:

- **Confidentiality:** Preserving authorized restrictions on information access and disclosure[2]. A loss of confidentiality is the unauthorized disclosure of information[3].
- **Integrity:** Guarding against improper information modification or destruction[4]. A loss of integrity is the unauthorized modification or destruction of information[5].
- **Availability:** Ensuring timely and reliable access to and use of information[6]. A loss of availability is the disruption of access to or use of information[7].

Q: What is the difference between a security attack, mechanism, and service?

A:

- **Security Attack:** Any action that compromises the security of information owned by an organization[8].
- **Security Mechanism:** A process (or device) designed to detect, prevent, or recover from a security attack[9].
- **Security Service:** A communication service that enhances the security of data processing systems and information transfers. It is intended to counter security attacks and uses one or more security mechanisms[10].

Q: What is the difference between passive and active security attacks?

A:

- **Passive Attacks:** Involve eavesdropping on or monitoring transmissions. The goal is to obtain information without modifying it[11]. The two types are **Release of message contents**[12] and **Traffic analysis**[13].
- **Active Attacks:** Involve some modification of the data stream or the creation of a false stream[14].

Q: (From Test Paper) Explain the Active Security attacks attack types in detail.

A: Active attacks involve modifying the data stream or creating a false one[15]. The four main categories are:

1. **Masquerade (Impersonation):** This takes place when one entity pretends to be a different entity[16]. An example is logging in using stolen credentials[17].
2. **Replay:** This involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect[18]. An example is reusing a payment request message to withdraw money a second time[19].
3. **Modification of messages:** This means that some portion of a legitimate message is altered, or messages are delayed or reordered, to produce an unauthorized effect[20]. An example is altering a message from "Allow John Smith to read..." to "Allow Fred Brown to read..."[21].
4. **Denial of Service (DoS):** This prevents or inhibits the normal use or management of communications facilities[22]. It can be done by disabling a network or overloading it with messages to degrade performance[23]. An example is flooding a server with requests so real users cannot log in[24].

Q: What are the two requirements for the secure use of conventional (symmetric) encryption?

A:

1. A **strong encryption algorithm** is needed. The opponent should be unable to decrypt the ciphertext or discover the key, even with access to multiple ciphertexts and their corresponding plaintexts[25].
2. The sender and receiver must **obtain copies of the secret key in a secure fashion** and must keep the key secure[26].

Q: (From Test Paper) Explain Caesar cipher and encrypt the text "Attack At Seven".

A:

- **Explanation:** The Caesar cipher is a substitution technique where each letter of the alphabet is replaced by the letter standing **three places further down** the alphabet[2727].
- The general algorithm is $C = E(k, p) = (p + k) \mod 26$, where p is the numerical value of the plaintext letter, k is the shift (key), and C is the numerical value of the ciphertext letter[2828]. For the standard Caesar cipher, the key k is 3[29292929].
- The decryption algorithm is $p = D(k, C) = (C - k) \mod 26$[30].
- **Encryption:**
    1. **Plaintext:** "Attack At Seven"
    2. **Convert to single case** (following the slide example meet me... $\rightarrow$ PHHW PH...[31]): "ATTACK AT SEVEN"
    3. **Apply $k=3$ shift:**
        - A (0) + 3 = **D** (3)
        - T (19) + 3 = **W** (22)
        - T (19) + 3 = **W** (22)
        - A (0) + 3 = **D** (3)
        - C (2) + 3 = **F** (5)
        - K (10) + 3 = **N** (13)
        - (space) $\rightarrow$ (space)
        - A (0) + 3 = **D** (3)
        - T (19) + 3 = **W** (22)
        - (space) $\rightarrow$ (space)
        - S (18) + 3 = **V** (21)
        - E (4) + 3 = **H** (7)
        - V (21) + 3 = **Y** (24)
        - E (4) + 3 = **H** (7)
        - N (13) + 3 = **Q** (16)
    4. **Ciphertext: "DWWDFN DW VHYHQ"**

Q: Explain the encryption rules for the Playfair Cipher.

A: The Playfair cipher uses a 5x5 matrix built from a keyword[32]. It encrypts plaintext by treating pairs of letters (digrams) as single units[33333333].

1. **Filler Letter:** Repeating plaintext letters in the same pair are separated with a filler letter, such as 'x'[34].

2. **Same Row:** If two plaintext letters fall in the same row, each is replaced by the letter to its **right**, with the first element of the row circularly following the last[35].
3. **Same Column:** If two plaintext letters fall in the same column, each is replaced by the letter **beneath** it, with the top element of the column circularly following the last[36].
4. **Rectangle:** Otherwise, each plaintext letter is replaced by the letter that lies in its **own row and the column occupied by the other** plaintext letter[37].

Q: How does the Vigenere Cipher work?

A: The Vigenere cipher is a **polyalphabetic substitution** cipher, meaning it uses multiple substitution alphabets[38383838].

1. It uses a **keyword**[39].
2. This keyword is repeated in a circular manner until it matches the length of the plaintext[40].
3. Each letter of the plaintext is then encrypted using the corresponding letter of the repeated key by referencing a **Vigenère square** (or table)[41414141].
4. Mathematically, the encryption is $E_i = (P_i + K_i) \mod 26$, where P_i is the plaintext letter and K_i is the corresponding keyword letter[42].

Unit 2: Block Ciphers, DES, & AES

Q: What is the difference between a Block Cipher and a Stream Cipher?

A:

- A **Stream Cipher** encrypts a digital data stream one bit or one byte at a time[43].
- A **Block Cipher** takes a block of plaintext (e.g., 64 or 128 bits) and treats it as a whole, producing a ciphertext block of equal length[44].

Q: Explain the concepts of Diffusion and Confusion.

A:

- **Diffusion:** This property dissipates the statistical structure of the plaintext across the ciphertext[45]. It is achieved by having each plaintext digit affect the value of many ciphertext digits[46]. This is generally done using **permutation (or transposition)**[47474747].
- **Confusion:** This property aims to make the relationship between the encryption key and the ciphertext as complex as possible[48]. This is achieved using **substitution**[49].

Q: (From Test Paper) With a neat diagram explain Feistel Encryption and Decryption algorithm.

A:

- **Feistel Encryption:** The Feistel cipher is a design structure used to build block ciphers like DES[50].
    1. The input plaintext block is split into two equal halves, a left half (L_0) and a right half (R_0) [51].
    2. The cipher then goes through multiple rounds (e.g., 16 rounds)[52].
    3. In each round i, the following operations occur:
        - The left half of the next round is set to be the right half of the current round: $L_i = R_{i-1}$[53].
        - The right half of the next round is calculated by taking the left half of the current round and XORing it with the output of a round function F: $R_i = L_{i-1} \oplus F(R_{i-1}, K_i)$[54].
    4. The function F is the round function (which provides confusion), and K_i is the subkey for that round[55].
    5. After the final round, a final swap of the left and right halves is performed to produce the ciphertext56.
    57
- Feistel Decryption: The decryption process uses the exact same algorithm as encryption58. The only difference is that the round subkeys ($K_1, K_2, ... K_{16}$) are applied in the reverse order (e.g., K_{16} is used in the first decryption round, K_{15} in the second, and so on)59.
  60

Q: (From Test Paper) Illustrate Avalanche Effect with example.

A:

- **Illustration:** The **Avalanche Effect** is a desirable property for any encryption algorithm[61]. It means that a small change in the input (either a single bit of the **plaintext** or a single bit of the **key**) should produce a significant change in the output **ciphertext**[62].
- **Example:** In DES, this effect is strong. A 1-bit change in the plaintext (e.g., changing 0000... to 1000...) results in, on average, 34 bits of the 64-bit ciphertext being different[63]. Similarly, changing one bit in the key while keeping the plaintext the same also results in a completely different ciphertext[64]. This prevents attackers from finding patterns or deducing the key by making small changes to the plaintext[65].

Q: What are the four transformation functions used in each round of AES?

A: AES does not use a Feistel structure; instead, it processes the entire data block in each round[6666]. Each round (except the last) consists of four stages:

1. **Substitute Bytes:** A non-linear byte-by-byte substitution using a predefined lookup table called an **S-box**[67676767].
2. **ShiftRows:** A simple permutation where the bytes in the last three rows of the 4x4 state matrix are cyclically shifted to the left by different offsets[68686868].
3. **MixColumns:** A transformation that operates on each column of the state individually, combining the four bytes in each column using arithmetic in $GF(2^8)$[69696969].
4. **AddRoundKey:** The state is bitwise XORed with the round key for that round[70707070].

Q: (From Test Paper) Illustrate the key expansion function of AES algorithm.

A:

The AES Key Expansion function generates a schedule of round keys from the initial cipher key71. The number of round keys needed depends on the number of rounds (e.g., 10 rounds for a 128-bit key)72.

The expansion for a 128-bit key (which is 4 words) works as follows:

- The first four words of the expanded key ($w[0]$ to $w[3]$) are the original cipher key[73].
- Every subsequent word $w[i]$ is generated by XORing the previous word $w[i-1]$ with the word from four positions back $w[i-4]$[74].
- **Special Step:** If i is a multiple of 4, a special function g is applied to $w[i-1]$ *before* the XOR. This g function consists of:
    1. **RotWord:** A one-byte circular left shift of the 4-byte word.
    2. **SubWord:** Each of the four bytes is passed through the AES S-box (the same one used in Substitute Bytes).
    3. **Rcon XOR:** The result is XORed with a **Round Constant (Rcon)**, which is a different value for each round[75].

This process ensures that each round key is unique and non-linearly related to the original cipher key76.

77

Unit 3: Public-Key Cryptography

Q: (From Test Paper) Explain the requirements of public key cryptography.

A: This topic, "Requirements for public-key cryptosystems," is listed as part of Unit III in the syllabus[78]. However, the provided documents (1.pdf, 2.pdf) do not contain the slides that explain these requirements in detail.

Q: (From Test Paper) Given p=7 and q=17, PT(Plaintext)=6, Find the value of e, d to form a public key and private key. What will be the Cipher text and again calculate text value from cipher text.

A: This question requires applying the **RSA algorithm**[79], which is part of Unit III. The provided documents list this topic in the syllabus[80] but do not contain the description of the algorithm, its formulas, or the computational steps needed to solve this problem.

Would you like me to create more questions based on specific topics, like security mechanisms or block cipher design principles?