Cryptography and Cyber Security Puzzle

Puzzle Scenario:

You are a cryptography expert working on a top-secret project. Your task is to solve a series of clues to recover a hidden message. Each clue involves a different aspect of the cryptography syllabus. Use the clues to decrypt the final hidden message.

Clue 1: Caesar Cipher

Clue: You find a note with the message “KHOOR ZRUOG”. The note is written using a Caesar Cipher with a shift of 3.

Task: Decrypt the message.

Answer: To decrypt, shift each letter back by 3 positions:

- K → H
- H → E
- O → L
- R → O
- Z → W
- U → R
- R → O
- O → L
- G → D

Decrypted Message: "HELLO WORLD"

Clue 2: Playfair Cipher

Clue: You have the keyword “SECURITY” and a message “MEET AT NOON”. The Playfair Cipher matrix is constructed using the keyword.

Task: Construct the matrix and encrypt the message. (Assume 'J' is omitted and replaced by 'I').

Matrix:

S E C U R

I T A B D

F G H K L

M N O P Q

V W X Y Z

Answer: Encrypting “MEET AT NOON”:

- M → M
- E → E
- E → E
- T → T
- A → A
- T → T
- N → N
- O → O
- O → O
- N → N

Using the matrix, the encrypted pairs are:

- ME → LE
- ET → OT
- AT → IY
- NO → MP
- ON → MM

Encrypted Message: "LEOT IY MPMM"

Clue 3: Hill Cipher

Clue: You are given a 2x2 key matrix and a plaintext “HI”. The key matrix is:

[2 3]

[1 4]

Task: Encrypt the plaintext using the Hill Cipher.

Answer: Convert “HI” to numerical vectors (H=7, I=8). Matrix multiplication:

[2 3] [7]

[1 4] * [8]

Results in:

[2*7 + 3*8, 1*7 + 4*8] = [34, 39]

Encrypted Message: "IN"

Clue 4: RSA Key Generation

Clue: To generate RSA keys, you choose two prime numbers: 7 and 11. Calculate the modulus nnn and the totient ϕ(n)\phi(n)ϕ(n).

Task: Compute the modulus nnn and the totient ϕ(n)\phi(n)ϕ(n).

Answer:

- n=7×11=77n = 7 \times 11 = 77n=7×11=77
- ϕ(n)=(7−1)×(11−1)=6×10=60\phi(n) = (7-1) \times (11-1) = 6 \times 10 = 60ϕ(n)=(7−1)×(11−1)=6×10=60

Modulus nnn: 77
Totient ϕ(n)\phi(n)ϕ(n): 60

Clue 5: Diffie-Hellman Key Exchange

Clue: Alice and Bob want to exchange keys using Diffie-Hellman with a prime modulus p=23p = 23p=23 and base g=5g = 5g=5. Alice chooses a private key a=6a = 6a=6 and Bob chooses a private key b=15b = 15b=15.

Task: Compute the shared secret key.

Answer:

1. Compute Alice's public key: A=gamod p=56mod 23=8A = g^a \mod p = 5^6 \mod 23 = 8A=gamodp=56mod23=8
2. Compute Bob's public key: B=gbmod p=515mod 23=2B = g^b \mod p = 5^{15} \mod 23 = 2B=gbmodp=515mod23=2
3. Compute shared key:
    - Alice computes: K=Bamod p=26mod 23=13K = B^a \mod p = 2^6 \mod 23 = 13K=Bamodp=26mod23=13
    - Bob computes: K=Abmod p=815mod 23=13K = A^b \mod p = 8^{15} \mod 23 = 13K=Abmodp=815mod23=13

Shared Secret Key: 13

Clue 6: DES Algorithm

Clue: Encrypt the plaintext “HELLO” using the DES algorithm with a simplified key. Assume a simplified DES that uses a key of 10101010.

Task: Describe the basic steps of DES encryption.

Answer: DES encryption involves the following steps:

1. **Initial Permutation:** Rearrange the plaintext.
2. **Key Schedule:** Generate 16 subkeys from the main key.
3. **Rounds:** Perform 16 rounds of Feistel function operations.
4. **Final Permutation:** Rearrange the data to obtain the ciphertext.

Note: This is a simplified explanation; real DES involves complex permutations and substitutions.

Clue 7: AES Encryption

Clue: Encrypt the plaintext “DATA” using AES with a 128-bit key. Assume a simple key for demonstration purposes.

Task: Describe the basic steps of AES encryption.

Answer: AES encryption involves the following steps:

1. **Key Expansion:** Generate a series of round keys from the original key.
2. **Initial Round:** Add the initial round key to the plaintext.
3. **Rounds:** Perform a series of transformations (SubBytes, ShiftRows, MixColumns, AddRoundKey) for 10 rounds.
4. **Final Round:** Perform SubBytes, ShiftRows, and AddRoundKey without MixColumns.

Note: Actual AES operations are performed on byte blocks and involve specific substitution tables and permutations.

Final Hidden Message

Combine all decrypted messages and solutions from the clues above to reveal the hidden message.

Clues Revealed:

1. "HELLO WORLD"
2. "LEOT IY MPMM"
3. "IN"
4. (RSA and DH answers are numerical; not part of final message)
5. (DES and AES descriptions are process steps; not part of final message)

Final Hidden Message: "HELLO WORLD LEOT IY MPMM IN"