Assignment 1

Q1) Given Plain Text: CRYPTO
represented as [2, 17, 24, 15, 19, 14]
key = SECRET
represented as [18, 4, 2, 17, 4, 19]

Ans $C_i = (P_i + k_i) \bmod 26$

$C_1 = (2+18) \bmod 26 = 20 = U$
$C_2 = (17+4) \bmod 26 = 21 = V$
$C_3 = (24+2) \bmod 26 = 0 = A$
$C_4 = (15+17) \bmod 26 = 6 = G$
$C_5 = (19+4) \bmod 26 = 23 = X$
$C_6 = (14+19) \bmod 26 = 7 = H$

Cipher Text = UVAGXH

Q2) Given Cipher Text: XMPWYQ
represented as [23, 12, 15, 22, 24, 16]
key = KEYPAD
represented as [10, 4, 24, 15, 0, 3]

Ans $C_i = P_i = (C_i - K_i) \bmod 26$

$P_1 = (23 - 10) \bmod 26 = 13 = N$

$P_2 = (12 - 4) \bmod 26 = 8 = I$

$P_3 = (15 - 24) \bmod 26 = -9 = 17 = R$

$P_4 = (22 - 15) \bmod 26 = 7 = H$

$P_5 = (24 - 0) \bmod 26 = 24 = Y$

$P_6 = (16 - 3) \bmod 26 = 13 = N$

NIRHYN

Q3) Reversibility

Prove that the encryption and decryption process in the one-time pad are mathematically reversible by showing that

$P(C-K) \bmod 26$

where $C = (P+K) \bmod 26$, P is plain text, C is cipher text, K is key

Encryption formula

$$C = (P + K) \bmod 26 \quad -(1)$$

To recover P, we apply decryption formula

$$P = (C - K) \bmod 26 \quad -(2)$$

Substituting C from encryption formula

$$P = (((P + K) - K) \bmod 26) - K) \bmod 26$$

$$P = ((P + K - K) \bmod 26) \bmod 26$$

$$P = (P \cdot \bmod 26) \bmod 26$$

$$\because P \bmod 26 = P$$

(as P is already between 0 & 25)

$$P = P$$

Hence, Proved, applying the decryption formula after encryption formula returns original Plaintext

Q4 If the plaintext has 8 characters and each character is represented as a number modulo 26, how many possible unique keys can be generated for encryption? Provide the result as a power of 26.

Ans. Given: Plaintext characters = 8
26 possible values (0-25)

key should be same length as the plaintext = 8 characters

For each of the 8 positions in the key, there are 26 possible choices

Total no. of possible keys:

$26^8 = 26 \times 26 \times 26 \times 26 \times 26 \times 26 \times 26 \times 26$

Q5] Two messages: P_1 and P_2 are encrypted using same key, resulting in ciphertext C_1 and C_2. Show mathematically how an attacker can compute $P1 \oplus P2$ from C_1 & C_2. Explain why this compromises security.

Ans Encryption for one-time pad

$$C = (P + k) \bmod 26$$

where P → plaintext
C → ciphertext

Encryption process

For P_1, C_1 will be

$$C_1 = (P_1 + k) \bmod 26$$

For P_2, C_2 will be

$$C_2 = (P_2 + k) \bmod 26$$

Attacker's Goal:

∴ Compute $C_1 \oplus C_2$ (∵ same key is used)

$C_1 \oplus C_2 = ((P_1 + k) \bmod 26 \oplus ((P_2 + k) \bmod 26)$

$C_1 \oplus C_2 = (P_1 + k) \oplus (P_2 + k) = (P_1 \oplus P_2) \bmod 26$

By XOR operation

$C_1 \oplus C_2 = P_1 \oplus P_2 \bmod 26$

attacker doesn't need to know the key to calculate $P_1 \oplus P_2$

If attacker know some part of $P_1 \oplus P_2$ they can easily deduce information about P_1 & P_2

The fact that XORing two ciphertexts yields the XOR of their corresponding fundamentally compromises security.

One-time pad are supposed to be secure as long as the key is random, used only once and is kept secret. Using same key for two messages allows an attacker to compute relationship between them, compromising the cryptosystem's confidentiality.