

مثال:

1. تشفير النص "HELLO" باستخدام المفتاح "KEY":

- النص الصريح:
"HELLO"
 - المفتاح:
"KEY"
-

خطوات التشفير:

1. تحويل الأحرف إلى أرقام:

- (A=0, B=1, ..., Z=25): استخدم جدول الأحرف الأبجدي:
 - النص الصريح:
H = 7, E = 4, L = 11, L = 11, O = 14
 - المفتاح:
K = 10, E = 4, Y = 24

2. إعادة استخدام المفتاح لتغطية النص الصريح بالكامل:

- النص الصريح: "HELLO"
- المفتاح المتكرر: "KEYKE"
(K=10, E=4, Y=24, K=10, E=4)

3. معادلة التشفير:

$$C = (P + K) \mod 26$$

حيث:

- هو الرقم المقابل للحرف في النص الصريح P .
- هو الرقم المقابل للحرف في المفتاح K .

4. حساب القيم لكل حرف:

- الحرف الأول (H):

$$C = (7 + 10) \mod 26 = 17 \quad (\text{الحرف: R})$$

- الحرف الثاني (E):

$$C = (4 + 4) \mod 26 = 8 \quad (\text{الحرف: I})$$

- الحرف الثالث (L):

$$C = (11 + 24) \mod 26 = 9 \quad (\text{الحرف: J})$$

- الحرف الرابع (L):

$$C = (11 + 10) \mod 26 = 21 \quad (\text{الحرف: V})$$

- الحرف الخامس (O):

$$C = (14 + 4) \mod 26 = 18 \quad (\text{الحرف: S})$$

5. النص المشفر:

Cipher Text = "RIJVS"

2. فك تشفير النص "RIJVS" باستخدام نفس المفتاح "KEY":

- النص المشفر:
"RIJVS"
- المفتاح:
"KEY"

خطوات فك التشفير:

1. تحويل الأحرف إلى أرقام:

- النص المشفر:
 $R = 17, I = 8, J = 9, V = 21, S = 18$
- المفتاح المتكرر:
 $K = 10, E = 4, Y = 24, K = 10, E = 4$

2. معادلة فك التشفير:

$$P = (C - K) \mod 26$$

حيث:

- C هو الرقم المقابل للحرف في النص المشفر
- K هو الرقم المقابل للحرف في المفتاح

3. حساب القيم لكل حرف:

- الحرف الأول (R):

$$P = (17 - 10) \mod 26 = 7 \quad (\text{الحرف: H})$$

حيث:

- C هو الرقم المقابل للحرف في النص المشفر
- K هو الرقم المقابل للحرف في المفتاح

3. حساب القيم لكل حرف:

- الحرف الأول (R):

$$P = (17 - 10) \bmod 26 = 7 \quad (\text{الحرف: H})$$

- الحرف الثاني (I):

$$P = (8 - 4) \bmod 26 = 4 \quad (\text{الحرف: E})$$

- الحرف الثالث (J):

$$P = (9 - 24) \bmod 26 = 11 \quad (\text{الحرف: L})$$

- الحرف الرابع (V):

$$P = (21 - 10) \bmod 26 = 11 \quad (\text{الحرف: L})$$

- الحرف الخامس (S):

$$P = (18 - 4) \bmod 26 = 14 \quad (\text{الحرف: O})$$

4. النص الصريح:

Plain Text = "HELLO"

النتيجة النهائية:

- "RIJVS" يصبح "HELLO" التشفير: النص
- "HELLO" يعود إلى "RIJVS" فك التشفير: النص