

مثال:

1. تشفير النص "Attack is today" باستخدام المفتاح الأولي $K_1 = 12$:

- النص الصريح:
"Attack is today"
- المفتاح الأولي:
 $K_1 = 12$

خطوات التشفير:

1. تحويل الأحرف إلى أرقام:

- استخدام جدول الأحرف الأبجدي ($A=0, B=1, \dots, Z=25$):

- النص الصريح:

$A = 0, T = 19, T = 19, A = 0, C = 2, K = 10, I = 8, S = 18, T = 19, O = 14, D = 3, A = 0, Y = 24$

2. إنشاء المفتاح الكامل:

- $K_1 = 12$ المفتاح الأولي هو.
- يتم إنشاء باقي المفتاح باستخدام النص الصريح نفسه:
 - 12, 0, 19, 19, 0, 2, 10, 8, 18, 19, 14, 3, 0

3. معادلة التشفير:

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

حيث:

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

4. حساب القيم لكل حرف:

- الحرف الأول (A):

$$C = (0 + 12) \mod 26 = 12 \quad (\text{الحرف: M})$$

- الحرف الثاني (T):

$$C = (19 + 0) \mod 26 = 19 \quad (\text{الحرف: T})$$

- الحرف الثالث (T):

$$C = (19 + 19) \mod 26 = 12 \quad (\text{الحرف: M})$$

- الحرف الرابع (A):

$$C = (0 + 19) \mod 26 = 19 \quad (\text{الحرف: T})$$

- الحرف الخامس (C):

$$C = (2 + 0) \mod 26 = 2 \quad (\text{الحرف: C})$$

- الحرف السادس (K):

$$C = (10 + 2) \mod 26 = 12 \quad (\text{الحرف: M})$$

- الحرف السابع (I):

$$C = (8 + 10) \mod 26 = 18 \quad (\text{الحرف: S})$$

- الحرف الثامن (S):

$$C = (18 + 8) \mod 26 = 0 \quad (\text{الحرف: A})$$

- الحرف التاسع (T):

$$C = (19 + 18) \mod 26 = 11 \quad (\text{الحرف: L})$$

- الحرف العاشر (O):

$$C = (14 + 19) \mod 26 = 7 \quad (\text{الحرف: H})$$

- الحرف الحادي عشر (D):

$$C = (3 + 14) \mod 26 = 17 \quad (\text{الحرف: R})$$

- الحرف الثاني عشر (A):

$$C = (0 + 3) \mod 26 = 3 \quad (\text{الحرف: D})$$

- الحرف الثالث عشر (Y):

$$C = (24 + 0) \mod 26 = 24 \quad (\text{الحرف: Y})$$

5. النص المشفر:

Cipher Text = "MTMTCMSALHRDY"

2. فك تشفير النص "MTMTCMSALHRDY" باستخدام نفس المفتاح الأولي $K_1 = 12$:

- النص المشفر:
"MTMTCMSALHRDY"
- المفتاح الأولي:
 $K_1 = 12$

خطوات فك التشفير:

1. تحويل الأحرف إلى أرقام:

- النص المشفر:

M = 12, T = 19, M = 12, T = 19, C = 2, M = 12, S = 18, A = 0, L = 11, H = 7, R = 17, D = 3, Y = 24

2. إعادة إنشاء المفتاح الكامل:

- $K_1 = 12$ المفتاح الأولي هو.
- يتم إعادة بناء المفتاح باستخدام النص الصريح الذي يتم فك تشفيره تدريجيًا.

3. معادلة فك التشفير:

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

حيث:

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

4. حساب القيم لكل حرف:

- الحرف الأول (M):

$$P = (12 - 12) \mod 26 = 0 \quad (\text{الحرف: A})$$

- الحرف الثاني (T):

$$P = (19 - 0) \mod 26 = 19 \quad (\text{الحرف: T})$$

- الحرف الثالث (M):

$$P = (12 - 19) \mod 26 = 19 \quad (\text{الحرف: T})$$

- الحرف الرابع (T):

$$P = (19 - 19) \mod 26 = 0 \quad (\text{الحرف: A})$$

- الحرف الخامس (C):

$$P = (2 - 0) \mod 26 = 2 \quad (\text{الحرف: C})$$

- الحرف السادس (M):

$$P = (12 - 2) \mod 26 = 10 \quad (\text{الحرف: K})$$

- الحرف السابع (S):

$$P = (18 - 10) \bmod 26 = 8 \quad (\text{الحرف: I})$$

- الحرف الثامن (A):

$$P = (0 - 8) \bmod 26 = 18 \quad (\text{الحرف: S})$$

- الحرف التاسع (L):

$$P = (11 - 18) \bmod 26 = 19 \quad (\text{الحرف: T})$$

- الحرف العاشر (H):

$$P = (7 - 19) \bmod 26 = 14 \quad (\text{الحرف: O})$$

- الحرف الحادي عشر (R):

$$P = (17 - 14) \bmod 26 = 3 \quad (\text{الحرف: D})$$

- الحرف الثاني عشر (D):

$$P = (3 - 3) \bmod 26 = 0 \quad (\text{الحرف: A})$$

- الحرف الثالث عشر (Y):

$$P = (24 - 0) \bmod 26 = 24 \quad (\text{الحرف: Y})$$

5. النص الصريح:

Plain Text = "Attack is today"

النتيجة النهائية:

- "MTMTCMSALHRDY" يصبح "Attack is today" التشفير: النص
 - "Attack is today" يعود إلى "MTMTCMSALHRDY" فك التشفير: النص
-