

1. تشفير النص "ALMO" باستخدام المفاتيح $K_1 = 7$ و $K_2 = 4$:

- النص الصريح: **ALMO**
- الخطوة الأولى: تحويل الأحرف إلى أرقام باستخدام جدول الأحرف الأبجدي ($A=0, B=1, \dots, Z=25$):
 - $A = 0$
 - $L = 11$
 - $M = 12$
 - $O = 14$
- معادلة التشفير:

$$C = (P \cdot K_1 + K_2) \mod 26$$

حيث:

- P هو الرقم المقابل للحرف في النص الصريح.
- K_1 و K_2 هما المفتاحان المستخدمان للتشفير.
- حساب القيم:
 - A ($P = 0$): للحرف

$$C = (0 \cdot 7 + 4) \mod 26 = 4 \mod 26 = 4 \quad (\text{الحرف: E})$$

- L ($P = 11$): للحرف

$$C = (11 \cdot 7 + 4) \mod 26 = (77 + 4) \mod 26 = 81 \mod 26 = 3 \quad (\text{الحرف: D})$$

- M ($P = 12$): للحرف

$$C = (12 \cdot 7 + 4) \mod 26 = (84 + 4) \mod 26 = 88 \mod 26 = 10 \quad (\text{الحرف: K})$$

- O ($P = 14$): للحرف

$$C = (14 \cdot 7 + 4) \mod 26 = (98 + 4) \mod 26 = 102 \mod 26 = 24 \quad (\text{الحرف: Y})$$

- النص المشفر:

Cipher Text = "EDKY"

2. فك تشفير النص "EDKY" باستخدام المعكوس النقطي للمفتاح K_1^{-1} :

- النص المشفر: **EDKY**
- الخطوة الأولى: تحويل الأحرف إلى أرقام:
 - E = 4
 - D = 3
 - K = 10
 - Y = 24
- معادلة فك التشفير:

$$P = (C - K_2) \cdot K_1^{-1} \mod 26$$

حيث:

- هو الرقم المقابل للحرف في النص المشفر C .
- هو المعكوس النقطي للمفتاح K_1 بالنسبة إلى 26 K_1^{-1} .
- إيجاد المعكوس النقطي لـ $K_1 = 7$:
 - نبحث عن رقم x بحيث:

$$(7 \cdot x) \mod 26 = 1$$

- لأن $x = 15$ هو الحل هو:

$$(7 \cdot 15) \mod 26 = 105 \mod 26 = 1$$

- حساب القيم:

- $E (C = 4)$ للحرف

$$P = ((4 - 4) \cdot 15) \mod 26 = (0 \cdot 15) \mod 26 = 0 \quad (\text{الحرف: A})$$

- $D (C = 3)$ للحرف

$$P = ((3 - 4) \cdot 15) \mod 26 = (-1 \cdot 15) \mod 26 = -15 \mod 26 = 11 \quad (\text{الحرف: L})$$

- $K (C = 10)$ للحرف

$$P = ((10 - 4) \cdot 15) \mod 26 = (6 \cdot 15) \mod 26 = 90 \mod 26 = 12 \quad (\text{الحرف: M})$$

- $Y (C = 24)$ للحرف

$$P = ((24 - 4) \cdot 15) \mod 26 = (20 \cdot 15) \mod 26 = 300 \mod 26 = 14 \quad (\text{الحرف: O})$$

- النص الصريح:

Plain Text = "ALMO"

النتيجة النهائية:

- "EDKY" يصبح "ALMO" التشفير: النص
- "ALMO" يعود إلى "EDKY" فك التشفير: النص

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:
 - المفتاح: $12, 0, 19, 19, 0, 2, 10, 8, 18, 19, 14, 3, 0$

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
-

Caesar Cipher

- Example:** suppose the key for a *shift cipher is $K = 13$* and the plaintext is

we go to INU



a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Plain text	w	e	g	o	t	o	i	n	u
Sequence	22	4	6	14	19	14	8	13	20
Cipher sequence ($p + 13$) mod 26	9	17	19	1	6	1	21	0	7
Cipher text	j	r	t	b	g	b	v	a	h

Cipher text: jrtbgbvah

Caesar Cipher

- **Example:** suppose the key for a **shift cipher is $K = 13$** and the cipher text is:

Cipher text: jrtbgbvah

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Cipher text	<u>i</u>	<u>r</u>	<u>t</u>	<u>b</u>	<u>g</u>	<u>b</u>	<u>v</u>	<u>a</u>	<u>h</u>
Sequence	<u>9</u>	<u>17</u>	19	1	6	1	21	0	<u>7</u>
Plain sequence	$(9-13) \bmod 26$	4	6	14	19	14	8	13	20
$(c - 13) \bmod 26$	22	$-4 \bmod 26 \rightarrow$							
Cipher text	w	e	g	o	t	o	i	n	u

plain text: we go to inu

$$-4 = -1 \times 26 + 22$$

مثال:

1. تشفير النص "PAY" باستخدام مصفوفة المفتاح:

- النص الصريح: **PAY**
- الخطوة الأولى: تحويل الأحرف إلى أرقام باستخدام جدول الأحرف الأبجدي (A=0, B=1, ..., Z=25):
 - P = 15
 - A = 0
 - Y = 24
- مصفوفة المفتاح (Key Matrix):

$$K = \begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix}$$

- النص الصريح كمتجه عمودي:

$$P = \begin{bmatrix} 15 \\ 0 \\ 24 \end{bmatrix}$$

- ضرب مصفوفة المفتاح في متجه النص الصريح:

$$C = K \cdot P \pmod{26}$$

$$C = \begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix} \cdot \begin{bmatrix} 15 \\ 0 \\ 24 \end{bmatrix} \pmod{26}$$

- حساب القيم:

- الصف الأول:

$$C_1 = (17 \cdot 15 + 17 \cdot 0 + 5 \cdot 24) \pmod{26} = (255 + 0 + 120) \pmod{26} = 375 \pmod{26} = 11$$

- الصف الثاني:

$$C_2 = (21 \cdot 15 + 18 \cdot 0 + 21 \cdot 24) \pmod{26} = (315 + 0 + 504) \pmod{26} = 819 \pmod{26} = 13$$

- الصف الثالث:

$$C_3 = (2 \cdot 15 + 2 \cdot 0 + 19 \cdot 24) \pmod{26} = (30 + 0 + 456) \pmod{26} = 486 \pmod{26} = 18$$

- النص المشفر كأرقام:

$$C = \begin{bmatrix} 11 \\ 13 \\ 18 \end{bmatrix}$$

- تحويل الأرقام إلى أحرف:
 - $11 = L$
 - $13 = N$
 - $18 = S$
- النص المشفر: **LNS**

2. فك تشفير النص "LNS" باستخدام مصفوفة المفتاح العكسي:

- النص المشفر: **LNS**
- الخطوة الأولى: تحويل الأحرف إلى أرقام:
 - $L = 11$
 - $N = 13$
 - $S = 18$
- مصفوفة المفتاح العكسي (Inverse Key Matrix):

$$K^{-1} = \begin{bmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{bmatrix}$$

- النص المشفر كمتجه عمودي:

$$C = \begin{bmatrix} 11 \\ 13 \\ 18 \end{bmatrix}$$

- ضرب مصفوفة المفتاح العكسي في متجه النص المشفر:

$$P = K^{-1} \cdot C \mod 26$$
$$P = \begin{bmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{bmatrix} \cdot \begin{bmatrix} 11 \\ 13 \\ 18 \end{bmatrix} \mod 26$$

- حساب القيم:

- الصف الأول

$$P_1 = (4 \cdot 11 + 9 \cdot 13 + 15 \cdot 18) \mod 26 = (44 + 117 + 270) \mod 26 = 431 \mod 26 = 15$$

- الصف الثاني:

$$P_2 = (15 \cdot 11 + 17 \cdot 13 + 6 \cdot 18) \mod 26 = (165 + 221 + 108) \mod 26 = 494 \mod 26 = 0$$

- الصف الثالث:

$$P_3 = (24 \cdot 11 + 0 \cdot 13 + 17 \cdot 18) \mod 26 = (264 + 0 + 306) \mod 26 = 570 \mod 26 = 24$$

- النص الصريح كأرقام:

$$P = \begin{bmatrix} 15 \\ 0 \\ 24 \end{bmatrix}$$

- تحويل الأرقام إلى أحرف:

- $15 = P$
- $0 = A$
- $24 = Y$

- النص الصريح: **PAY**

النتيجة النهائية:

- "LNS" يصبح "PAY" **التشفير**: النص
- "PAY" يعود إلى "LNS" **فك التشفير**: النص

1. تشفير النص "ALMO" باستخدام المفتاح $K = 9$:

- النص الصريح: **ALMO**
- الخطوة الأولى: تحويل الأحرف إلى أرقام باستخدام جدول الأحرف الأبجدي ($A=0, B=1, \dots, Z=25$):
 - $A = 0$
 - $L = 11$
 - $M = 12$
 - $O = 14$
- معادلة التشفير:

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

حيث:

- P هو الرقم المقابل للحرف في النص الصريح.
- K هو المفتاح المستخدم للتشفير.
- حساب القيم:
 - $A (P = 0)$ للحرف

$$C = (0 \cdot 9) \mod 26 = 0 \mod 26 = 0 \quad (\text{الحرف: A})$$

- $L (P = 11)$ للحرف

$$C = (11 \cdot 9) \mod 26 = 99 \mod 26 = 21 \quad (\text{الحرف: V})$$

- $M (P = 12)$ للحرف

$$C = (12 \cdot 9) \mod 26 = 108 \mod 26 = 4 \quad (\text{الحرف: E})$$

- $O (P = 14)$ للحرف

$$C = (14 \cdot 9) \mod 26 = 126 \mod 26 = 22 \quad (\text{الحرف: W})$$

- النص المشفر:

Cipher Text = "AVEW"

2. فك تشفير النص "AVEW" باستخدام المفتاح العكسي $K^{-1} = 3$:

- النص المشفر: **AVEW**
- الخطوة الأولى: تحويل الأحرف إلى أرقام:
 - $A = 0$
 - $V = 21$
 - $E = 4$
 - $W = 22$
- معادلة فك التشفير:

$$P = (C \cdot K^{-1}) \mod 26$$

حيث:

- هو الرقم المقابل للحرف في النص المشفر C .
- هو المعكوس النقطي للمفتاح K بالنسبة إلى 26 K^{-1} .
- حساب القيم:
 - $A (C = 0)$ للحرف

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

- $V (C = 21)$ للحرف

$$P = (21 \cdot 3) \mod 26 = 63 \mod 26 = 11 \quad (\text{الحرف: L})$$

- $E (C = 4)$ للحرف

$$P = (4 \cdot 3) \mod 26 = 12 \mod 26 = 12 \quad (\text{الحرف: M})$$

- $W (C = 22)$ للحرف

$$P = (22 \cdot 3) \mod 26 = 66 \mod 26 = 14 \quad (\text{الحرف: O})$$

- النص الصريح:

Plain Text = "ALMO"

النتيجة النهائية:

- "AVEW" يصبح "ALMO" التشفير: النص
- "ALMO" يعود إلى "AVEW" فك التشفير: النص

مثال:

1. تشفير النص "HELLO" باستخدام مفتاح عشوائي:

- النص الصريح:
"HELLO"
- المفتاح العشوائي (Random Key):
"XMCKL"

1. تحويل الأحرف إلى أرقام:

- استخدم جدول الأحرف الأبجدي ($A=0, B=1, \dots, Z=25$):
 - النص الصريح:
 $H = 7, E = 4, L = 11, L = 11, O = 14$
 - المفتاح:
 $X = 23, M = 12, C = 2, K = 10, L = 11$

2. معادلة التشفير:

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

حيث:

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

3. حساب القيم لكل حرف:

- الحرف الأول (H):

$$C = (7 + 23) \mod 26 = 30 \mod 26 = 4 \quad (\text{الحرف: E})$$

- الحرف الثاني (E):

$$C = (4 + 12) \mod 26 = 16 \quad (\text{الحرف: Q})$$

- الحرف الثالث (L):

$$C = (11 + 2) \mod 26 = 13 \quad (\text{الحرف: N})$$

- الحرف الرابع (L):

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

- الحرف الخامس (O):

$$C = (14 + 11) \mod 26 = 25 \quad (\text{الحرف: Z})$$

4. النص المشفر:

Cipher Text = "EQNVZ"

2. فك تشفير النص "EQNVZ" باستخدام نفس المفتاح "XMCKL":

- النص المشفر:
"EQNVZ"
- المفتاح:
"XMCKL"

1. تحويل الأحرف إلى أرقام:

- النص المشفر:

$$E = 4, Q = 16, N = 13, V = 21, Z = 25$$

- المفتاح:

$$X = 23, M = 12, C = 2, K = 10, L = 11$$

2. معادلة فك التشفير:

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

حيث:

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

3. حساب القيم لكل حرف:

- الحرف الأول (E):

$$P = (4 - 23) \mod 26 = -19 \mod 26 = 7 \quad (\text{الحرف: H})$$

- الحرف الثاني (Q):

$$P = (16 - 12) \mod 26 = 4 \quad (\text{الحرف: E})$$

- الحرف الثالث (N):

$$P = (13 - 2) \mod 26 = 11 \quad (\text{الحرف: L})$$

- الحرف الرابع (V):

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

- الحرف الخامس (Z):

$$P = (25 - 11) \mod 26 = 14 \quad (\text{الحرف: O})$$

4. النص الصريح:

Plain Text = "HELLO"

4. النص الصريح:

Plain Text = "HELLO"

النتيجة النهائية:

- "EQNVZ" يصبح "HELLO" **التشفير**: النص
- "HELLO" يعود إلى "EQNVZ" **فك التشفير**: النص

1. تشفير النص "ALMAMON UNIVERSITY COLLEGE" باستخدام المفتاح "231":

- النص الصريح:
"ALMAMON UNIVERSITY COLLEGE"
- المفتاح:
"231" (يحدد ترتيب الأعمدة)

خطوات التشفير:

1. ترتيب النص في جدول بناءً على المفتاح:

- قسّم النص إلى صفوف بحيث يكون عدد الأعمدة مساوياً لطول المفتاح (3 أعمدة هنا).
- لتكملة الجدول ("X" مثل) إذا كان النص لا يملأ الجدول بالكامل، يمكن إضافة حروف زائدة.

الجدول بعد ترتيب النص:

العمود 1	العمود 2	العمود 3
A	L	M
A	M	O
N	U	N
I	V	E
R	S	I
T	Y	C
O	L	L
E	G	E

2. إعادة ترتيب الأعمدة بناءً على المفتاح:

- المفتاح "231" يعني أن العمود الثاني يأتي أولاً، ثم العمود الثالث، ثم العمود الأول.
- الجدول بعد إعادة الترتيب:

العمود 1	العمود 3	العمود 2	⬇
A	M	L	
A	O	M	
N	N	U	
I	E	V	
R	I	S	
T	C	Y	
O	L	L	
E	E	G	

3. قراءة النص المشفر من الأعمدة الجديدة:

- اقرأ النص بشكل عمودي بدلاً من أفقي

Copy

```
1 LMNIRTOEX/MOUVSYLGX/AAONEICLE
```

- النص المشفر النهائي:

Copy

```
1 LMNIRTOEX/MOUVSYLGX/AAONEICLE
```

2. فك تشفير النص "LMNIRTOEX/MOUVSYLGX/AAONEICLE" باستخدام نفس المفتاح "231":

- النص المشفر:

Copy

```
1 LMNIRTOEX/MOUVSYLGX/AAONEICLE
```

- خطوات فك التشفير:

1. إعادة ترتيب النص في جدول بناءً على المفتاح:

- نعلم أن المفتاح "231" يعني أن العمود الثاني جاء أولاً، ثم العمود الثالث، ثم العمود الأول.
- نعيد الأعمدة إلى ترتيبها الأصلي بناءً على المفتاح.

الجدول بعد إعادة الترتيب:

العمود 1	العمود 2	العمود 3	↓
A	L	M	
A	M	O	
N	U	N	
I	V	E	
R	S	I	
T	Y	C	
O	L	L	
E	G	E	

2. قراءة النص الأصلي من الجدول:

- اقرأ النص بشكل أفقي:

```
1  ALMAMON UNIVERSITY COLLEGE
```

Copy

- النص الصريح النهائي:

```
1  ALMAMON UNIVERSITY COLLEGE
```

Copy

النتيجة النهائية:

- يصبح "ALMAMON UNIVERSITY COLLEGE" التشفير: النص

```
1  LMNIRTOEX/MOUVSYLGX/AAONEICLE
```

Copy

- يعود إلى "LMNIRTOEX/MOUVSYLGX/AAONEICLE" فك التشفير: النص

```
1  ALMAMON UNIVERSITY COLLEGE
```

Copy

مثال:

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

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

خطوات التشفير:

1. تحويل الأحرف إلى أرقام:

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

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

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

Group A

Q 1/ What will happen if your computer gets hacked?

- Hides programs
 - Generates unwanted traffic
 - Sends illegal software
 - Steals personal data
 - Records keystrokes (passwords)
-

Q2/

Given:

1. **Plain text** : "DE"

2. **Key** :

- $k_1 = 'B'$
- $k_2 = m_2m_3m_4m_5m_6m_7m_1$ (a transposition rule)

Step 1: Convert Plain Text to Binary

Each character in the plain text is converted into its ASCII binary representation:

- D : ASCII value = 68 $\rightarrow$ Binary = 1000100
- E : ASCII value = 69 $\rightarrow$ Binary = 1000101

Step 2: Convert Key $k_1 = 'B'$ to Binary

The key $k_1 = 'B'$ has an ASCII value of 66 $\rightarrow$ Binary = 1000010.

Step 3: Apply XOR Operation ($E_k^{(1)}$)

Perform XOR between the plain text and the key k_1 for each bit:

For D (1000100):

$$1000100 \oplus 1000010 = 0000110$$

For E (1000101):

$$1000101 \oplus 1000010 = 0000111$$

After XOR, the intermediate result is:

$$\text{Intermediate cipher (binary)} = 0000110\ 0000111$$

Step 4: Apply Transposition Rule ($E_k^{(2)}$)

The transposition rule $k_2 = m_4m_5m_6m_7m_1m_2m_3$ rearranges the bits of each 7-bit block as follows:

- Take the 4th, 5th, 6th, 7th, 1st, 2nd, and 3rd bits in that order.

For 0000110:

Original: 0000110

Rearranged: 0110000

For 0000111:

Original: 0000111

Rearranged: 0111000

After transposition, the final cipher text (in binary) is:

$$\text{Cipher text (binary)} = 0110000\ 0111000$$

Step 5: Convert Back to Characters

Convert the binary cipher text back to ASCII characters:

- 0110000: Binary = 0110000 $\rightarrow$ Decimal = 48 $\rightarrow$ Character = '0'
- 0111000: Binary = 0111000 $\rightarrow$ Decimal = 56 $\rightarrow$ Character = '8'

Group A

Q1 / State the Cautions when using Social Network

- 1. Privacy Concerns**
- 2. Cybersecurity Risks**
- 3. Misinformation and Fake News**
- 4. Online Harassment and Cyberbullying**
- 5. Addiction and Time Management**
- 6. Reputation Management**
- 7. Data Collection and Targeted Advertising**
- 8. Legal and Ethical Considerations**
- 9. Social Engineering Attacks**
- 10. Impact on Relationships**

Q2 / Encrypt the message "Hello Bob" By using Palyfair cipher if you have Key = "OCCURRENCE"

Solve :

1. إزالة الأحرف المكررة من المفتاح:
 - OCCURRENCE → OCUREN
2. إضافة باقي الحروف الأبجدية (باستثناء "J"):
 - الحروف المتبقية: A, B, D, F, G, H, I, K, L, M, P, Q, S, T, V, W, X, Y, Z
3. دمج الأحرف الفريدة للمفتاح مع الحروف المتبقية:
 - OCUREN + A, B, D, F, G, H, I, K, L, M, P, Q, S, T, V, W, X, Y, Z
4. ملء الشبكة 5x5 صفًا بصف:

1	O	C	U	R	E
2	N	A	B	D	F
3	G	H	I	K	L
4	M	P	Q	S	T
5	V	W	X	Y	Z

الخطوة 2: إعداد النص الصريح

النص الصريح هو "Hello bob". لتجهيزه للتشفير:

1. تحويل جميع الأحرف إلى أحرف كبيرة: "HELLO BOB".
2. استبدال "J" بـ "I" (إذا وُجد). في هذه الحالة، لا يوجد "J".
3. تقسيم النص إلى أزواج حرفية (Digraphs):
 - بينهما "X" إذا كانت الزوجة تحتوي على نفس الحرف، نضيف
 - في النهاية "X" إذا كان عدد الأحرف فرديًا، نضيف

النص الصريح: "HELLO BOB"

- التقسيم: HE LL OB OB
- تعديل الأزواج المكررة: HE LX LO BO BX

الأزواج النهائية: HE, LX, LO, BO, BX

الخطوة 4: دمج الأزواج المشفرة

دمج الأزواج المشفرة: LC, IZ, GE, NU, IU

الرسالة المشفرة: LCIZGENUIU

Q3/ Draw the sub key generation key algorithm in DES?

```
1  Input: 64-bit Key
2      ↓
3      Remove Parity Bits (8 bits ignored)
4      ↓
5      56-bit Key
6      ↓
7      PC-1 Permutation (Split into C0 and D0)
8      ↓
9      C0 (28 bits) _____|
10     |
11     D0 (28 bits) _____|
12     |
13     ↓
14     Round 1: Left Shift (1 or 2 bits)
15     ↓
16     C1, D1 _____|
17     |
18     PC-2 Permutation (Compression)
19     ↓
20     Subkey K1 (48 bits)
21     |
22     Repeat for 16 Rounds _____|
23     ↓
23     Output: 16 Subkeys (K1, K2, ..., K16)
```

Group C

Q1/ Explain the Trapdoors :

Trapdoors are hidden methods that allow bypassing security measures, often secretly embedded for legitimate (e.g., maintenance) or malicious (e.g., unauthorized access) purposes. They pose significant security risks if discovered.

Q2 / Find the Cipher text for the plain text "VERN" using the key = ' 76 48 16 82 ' , and Vernam cipher algorithm.

Step 1: Convert plaintext "VERN" to ASCII binary

Each character in "VERN" is converted to its 8-bit ASCII binary representation:

- **V** = 86 → 01010110
- **E** = 69 → 01000101
- **R** = 82 → 01010010
- **N** = 78 → 01001110

So, the binary representation of "VERN" is:

1 01010110 01000101 01010010 01001110

Copy

Step 2: Convert the key '76 48 16 82' to binary

Each number in the key is converted to its 8-bit binary representation:

- 76 → 01001100
- 48 → 00110000
- 16 → 00010000
- 82 → 01010010

So, the binary representation of the key is:

```
1 01001100 00110000 00010000 01010010
```

Copy

Step 3: Perform XOR operation between plaintext and key

We perform a bitwise XOR operation between the binary plaintext and the binary key.

For V (01010110) XOR 76 (01001100):

Copy

```
1  01010110
2  XOR 01001100
3  -----
4  = 00011010
```

For E (01000101) XOR 48 (00110000):

Copy

```
1  01000101
2  XOR 00110000
3  -----
4  = 01110101
```

For R (01010010) XOR 16 (00010000):

```
1  01010010
2  XOR 00010000
3  -----
4  = 01000010
```

For N (01001110) XOR 82 (01010010):

```
1  01001110
2  XOR 01010010
3  -----
4  = 00011100
```

00011010 01110101 01000010 00011100

Q3/ state the difference between block cipher and stream cipher .

- **Block Cipher** : Encrypts fixed-size blocks of data (e.g., 64 or 128 bits) at a time.
- **Stream Cipher** : Encrypts data one bit or byte at a time using a keystream.

Key Difference : Block ciphers work on chunks, stream ciphers work on continuous data flow.

Group D

Q1/ State the Types of service problems

1. Availability Problems
2. Quality Problems
3. Responsiveness Problems
4. Communication Problems
5. Accessibility Problems
6. Reliability Problems
7. Customization Problems
8. Billing and Pricing Problems
9. Technical Problems
10. Customer Service Problems
11. Security and Privacy Problems
12. Cultural or Language Barriers
13. Post-Service Problems

Q2/ Find the cipher text for the Plain text = "CDA" , by using the hill cipher algor