المحاضرة الخامسة:

خوارزمية الابدال العمودي Column Transposition Algorithm:

خطوات الإبدال العمودي كالآتي:

1- استخدام الترتيب للمسار العمودي.
2- اختيار مفتاح عدد رموزه بقدر عدد أعمدة النص الصريح.
3- إعادة ترتيب الأعمدة اعتمادا على المفتاح.
4- نحصل على النص المشفر من المصفوفة الأخيرة بعد تطبيق المفتاح ونقرأ من اليسار سطر سطر

Example: Encrypt by using column transposition algorithm the following text:

Plain text: **send help soon**

(1)	(2)	(3)	(4)
s	d	l	o
e	h	p	o
n	e	s	n

Choose a key: ⟹ Key= 2 4 3 1

ثم يتم التبديل بالأعمدة بما يشبه المفتاح كالآتي:

تقرأ من اليسار الى اليمين

(2)	(4)	(3)	(1)
d	o	l	s
h	o	p	e
e	n	s	n

ثم نأخذ النص المشفر من آخر مصفوفة

Cipher text: dolshopeensn

لفك الشفرة

نعود للنص **المشفر وبنفس المفتاح (يعاد الترتيب حسب المفتاح).**

ملاحظة:

إذا كان لدينا الحالة التالية (وهي ان ارقام المفتاح خارج نطاق الأعمدة) مثل

Key= 3 5 2 7 Or Key= 1 9 7 0

ففي مثل هذه الحالة نأخذ المفتاح الى اليمين وأقل رقم يحصل على أول تسلسل وهكذا:

Key = 1 9 7 0 ⟹ (1) (2) (3) (4)

New Key = 2 4 3 1

أما اذا كان المفتاح بشكل **حروف** فحسب تسلسلها الأبجدي تعاد صياغة المفتاح:

Key= F I G H T

New Key : 1 4 2 3 5

Double Column Transposition Algorithm: إبدال عمودي مزدوج

هذه الحالة مشابهة للحالة السابقة لكن بأخذ مفتاحين الأول نحصل منه على مصفوفة ثم نطبق عليها المفتاح الثاني فنحصل على المصفوفة النهائية ثم نستخرج النص المشفر

Application of column transposition to message (Twice). Two different keys are used, or the same key.

Example:

Encrypt the following message by using double column transposition if you know that:

K1= 3 1 4 2

K2= l o n g = 2 4 3 1

Plain text: send help soon

Then

s	d	l	o	نطبق المفتاح الأول	l	s	o	d
e	h	p	o	⟹	p	e	o	h
n	e	s	n	نحصل على k1	s	n	n	e

نطبق عليه المفتاح الثانى k2 ⟹ l o n g

النص المشفر النهائي

l	s	o	d	نطبق المفتاح الثاني	s	d	o	l
p	e	o	h	⟹	e	h	o	p
s	n	n	e	نحصل على k2	n	e	n	s

Cipher text: sdolehopnens

1- Polyliteral Transposition الابدال الحرفي المتعدد

هنا في هذه الطريقة نتعامل مع حرفين حرفين او ثلاثة حروف حسب التحديد أي كل موقع عبارة عن حرفين. ثم نطبق عليهم الابدال العمودي Column Transposition Algorithm

Example: Encrypt the following message by using Polyliteral Transposition Algorithm for

Plain text: Computer Sciences Department

␣ ␣

Then

co	er	nc	pa	nt
mp	sc	es	rt	xx
ut	ie	de	me	xx

ملاحظة:

إذا كان العدد للأحرف بعد الدمج لا يكفي لإكمال المصفوفة نضع XX (هنا x عبارة عن أي حرف يتم اختياره من قبل الشخص المشفر أي مصمم الشفرة) الى ان تكتمل المصفوفة.

الآن لدينا المفتاح

Key= F I G H T

1 4 2 3 5

اذن بتطبيق المفتاح نحصل على النص المشفر C كالآتي:

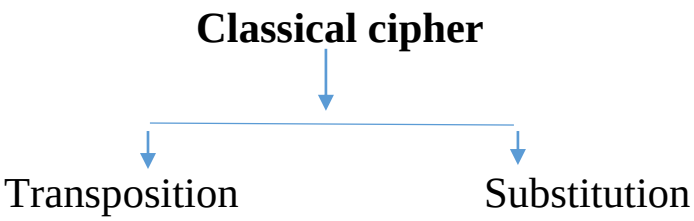
co	pa	er	nc	nt
mp	rt	sc	es	xx
ut	me	ie	de	xx

Cipher text: copaerncnt mprtscesxx utmeiedexx

H.W. **واجب**

Encrypt the following message by using Polyliteral Transposition Algorithm for

Plain text: send help soon



Substitution Ciphers: **الشفرات التعويضية**

In general, **replace** the character of message **with another one**.

الشفرات التعويضية: تبديل او تعويض حرف او رمز مكان الآخر لاي نص او رسالة صريحة

1- Direct standard (Caesar Cipher) شفرة قيصر او الشفرة المباشرة

2- Reciprocal (Reversal) Cipher الشفرة العكسية

3-Multiplicative Cipher الشفرة الضربية

4- Affine Cipher (Direct+ Multiplicative) شفرة افين

5- Mixed alphabet مزج الهجائيات

6- Key word Mixed (Key phrase) مزج الكلمة المفتاحية

7-Transposed keyword Mixed مزج الكلمة المفتاحية الابدالية