المحاضرة الثالثة:

Classical (Conventional) Systems:

It divided into two classes:

First: Transposition إبدال

Second: Substitution تعويض

First (Transposition): A rearrange or reorder the characters of plain text to get cipher text.

Example: By using message reversal algorithm encrypt the following

message?

(Plain text) P: send help soon.

(Cipher text) C: noos pleh dnes.

(b) Route Transposition Algorithm:

Plain text: send help soon

If the message have 12 letters we can write:

(2*6); (4*3); (3*4) … etc.

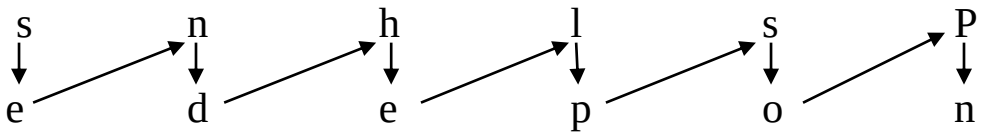
3*4	4*3	6*2
s e n d	s h s	s l
h e l p	e e o	e p
s o o n	n l o	n s
	d p n	d o
		h o
		e n

Note:

في حالة كون عدد حروف النص الصريح **فرديا** يمكن اضافة حرف زائد (pad character) ويفضل استخدام الرمز * لهذا الغرض.

1- Zig-Zag Route Transposition Algorithm:

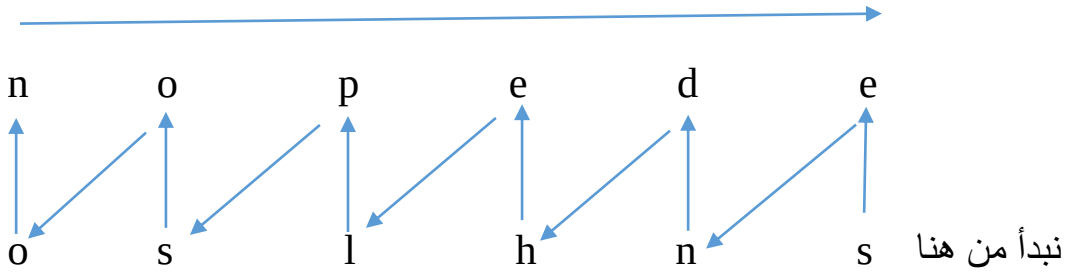
لنفس النص الصريح: تكتب أحرف النص على شكل **متعرج** ثم يؤخذ النص المشفر سطر سطر ومن اليسار الى اليمين اذن لنفس النص السابق:



الشكل اعلاه يمثل مصفوفة (2*6)

Cipher text: snhlso edepon

2- Reversalعكس (Anti Zig-Zag) Route Transposition Algorithm:



Cipher text C: nopede oslhns

3- Horizontal Route Transposition Algorithm:

هنا يتم كتابة النص بشكل **افقي** من أعلى اليسار ثم تعاد كتابة النص افقيا من أسفل اليمين ويقرأ من اليسار الى اليمين:

S* s e n d

h e l p

s o o o *e

Cipher

e* n o o s

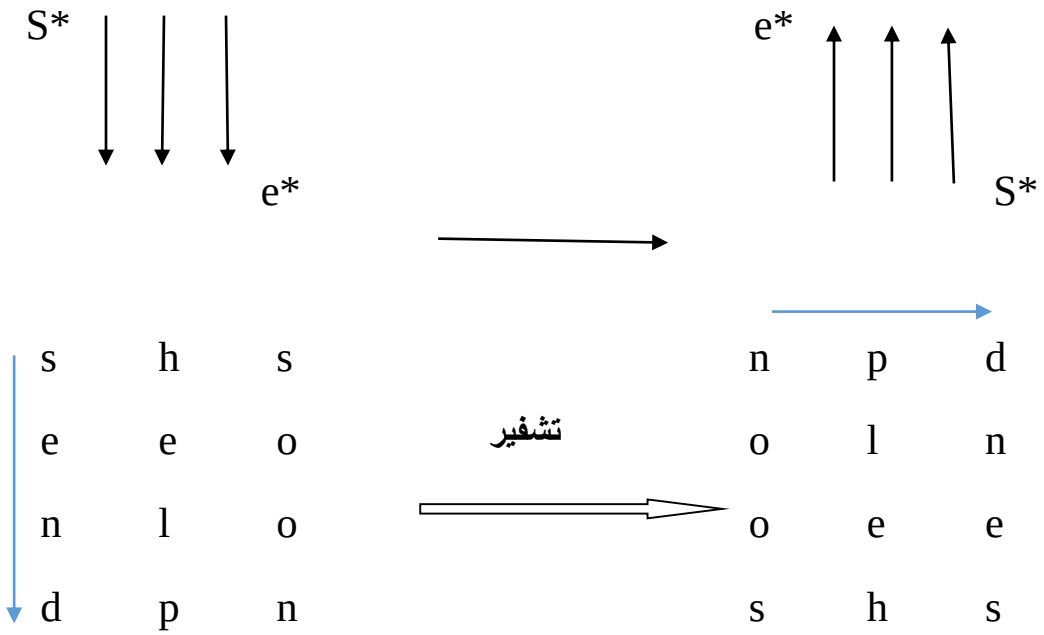
p l e h من هنا

d n e s S*

Plain text: send help soon ⟹ Cipher text: noos pleh dnes

4- Vertical Route Transposition Algorithm:

عبارة عن مصفوفة وتكتب بشكل **عمودي** وتعاد بشكل عمودي وتقرا من الأسفل



Cipher text: npd oln oee shs

ملاحظة مهمة: في الكتب الحديثة يكتب النص المشفر بدون فواصل للأمان **لجميع** خوارزميات التشفير كالآتي

Cipher text: npdolnoeeshs

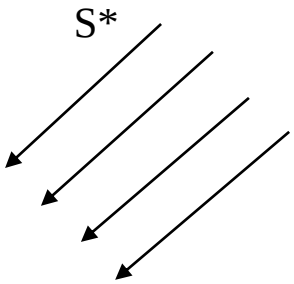
Example: If the matrix 4x3 becomes 3x4 then by vertical route:

s	d	l	o	n	s	e	n
e	h	p	o	o	p	h	e
n	e	s	n	o	l	d	s

Cipher text : nsenopheolds

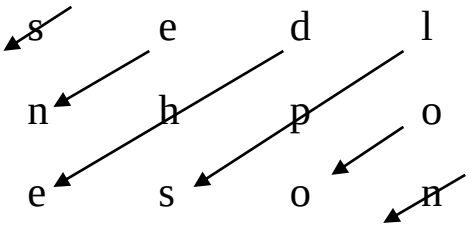
5- Diagonal Route Transposition Algorithm:

تكتب هذه الرسالة بشكل قطري كالآتي:

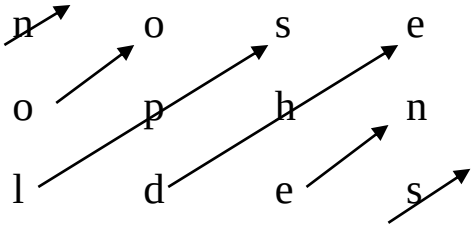


Example:

Plain text: send help soon



وتقرأ من اليسار الى اليمين



Cipher text: noseophnldes