

transposition technique

→ Consider the key as Computer.

P.t : attack postponed to tomorrow.

write the cipher text.

Sol:

computer.  
1 4 3 5 8 7 2 6

تسلسل كل حرف حسب الأولوية من الأجدية. يتم رقم key.

تسلسل مواقع الصفوف (ترتيباً). ←

key	1	2	3	4	5	6	7	8
1	4	3	5	8	7	2	6	
a	t	t	a	c	k	p	o	
s	t	p	o	n	e	d	t	
o	t	o	m	o	r	r	o	
w	x	x	x	x	x	x	x	

الفتاح هو الذي يحدد عدد الأعمدة وفي هذا المثال عدد الأعمدة 8  
الفتح لدينا صفوف 5 أعمدة.

عمود عمود  
تسلسل  
ارتفاع الفتح  
يتم C.t

حسب رقم الفتح  
العمود الأول

asow pdrx tpoxtttx aomx  
otox kerx onox

Column order : 1 7 3 2 4 8 6 5

حسب تسلسل الصفوف



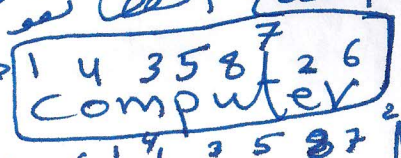
the description write the receiver etc  
 in the Form of Column and read the  
 Form on row according the order of  
 Secret key.

2

1	2	3	4	5	6	7	8
a	P	t	t	a	o	k	c
s	d	P	t	o	t	e	n
o	r	o	t	m	e	r	o
w	x	x	x	x	x	x	x

حقیقت

و یہ ترتیب افقی اظہار نقوم با استخراج p.t.  
 علیٰ ان افقی افقی  
 attack postponed to tomorrow



wxxxxxxx

وہذا یتم استخراج p.t.

نقوم بقراءة هذه والصيغة حقیقت والتماردا علی  
 ارجاء افقی. الیہ ( 1 4 3 5 8 7 2 6 )

مثلاً: (1) رقم (1) من الصف الاول هو  
 رقم (4) من الصف الاول هو t  
 رقم (3) من الصف الاول هو t  
 رقم (5) من الصف الاول هو a

وهذا.



# Data Encryption Standard (DES) algorithm.

→ is a symmetric algorithm, Block cipher takes 64 bit plain text, 56 bit key generates, 64 bit cipher text. 3

→ it contains 19 steps with 16 rounds and the

First step is taking 64 bit P.t and according to ~~the~~ initial transposition.

these bits divided into two groups

known as left block ( $L_{i-1}$ ) and Right block ( $R_{i-1}$ ). → (32-bit each blocks)

→ after transposition of these bits 16 rounds

are performed along with iteration key. at the end of 16 rounds the 64 bit data is being swapped as 32-bit swapping.

↓  
تبادل 32 بیتوں کے ساتھ  
تبادل فی ایٹم .