*transposition technique:-

→ Consider the key as computer.

P.t : attack postponed to tomorrow.

write the ciphar text.

Sol:

computer: 2
1 4 3 5 8 7 2 6

حسب تسلسل كل حرف حسب الأولوية من الأبجدية. ثم ترقيم الـ key.

تسلسل مواقع الصفوف (ترتيبا فقط).

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
P.t.	s	t	p	o	n	e	d	t
	o	t	o	m	o	r	r	o
	w	x	x	x	x	x	x	x

المفتاح هو الذي يحدد عدد الأعمدة في هذا المثال عدد أرقام المفتاح 8 إذن لدينا 8 صفوف و 8 أعمدة.

ترقيم المفتاح حسب الأولوية ⟹ العمود الأول

حسب ترتيب الثاني ⟹ الثاني

حسب ترتيب الثالث ⟹ الثالث. المفتاح

عمود عمود حسب تسلسل أرقام المفتاح. ينتج لـ c.t

asow pdrx tpox tttx aomx

otox kerx cnox.

[Column order: 1 7 3 2 5 4 8 6.]

حسب تسلسل الصفوف.

…e descryption write the receiver e.t 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	o	r	o
w	x	x	x	x	x	x	x

وحسب ترتيب المفتاح الخطأ نقوم باسترجاع الـ p.t. صفاً صفاً.

علماً ان المفتاح computer (1 4 3 5 8 7 2 6) حسب هذا الترتيب.

attack postponed to tomorro

w x x x x x x x

وهكذا يتم استخراج الـ p.t.

نقوم بقراءة هذه المصفوفة صفاً صفاً واعتماداً على تسلسل ارقام المفتاح. التي هي (1 4 3 5 8 7 2 6)

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

وهكذا.

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

↓

بحيث تكون L_{i-1} تحل محل R_{i-1}

يعني تبادل في البلوك.