Use of permutation in ciphers

in	out
1	3
2	7
3	2
4	5
5	1
6	4
7	6

knights

hiktgsn

theknights|lost|bythirty|sevenx

netikgh

no "real" encryption, just reordering.

Claude Shannon – father of information theory

"confusion and diffusion" (for good crypto)

↓ confusion: substitution

↓ diffusion: reordering + making multiple items of plaintext affect multiple items of ciphertext.

Column Permutation

keyword: APPLE (1 4 5 3 2)

T	O	D	A	Y
I	S	S	E	P
T	E	M	B	E
R	T	W	E	L
U	T	H	X	X

start next

1 → 11 (could be row 2, col 4 if 2nd keey is length 7

Cipher: TITRUYPELXAEBEX

OSETTDSMWH.

Read each column in the numbered order given above.

Double Transposition

Just applying transposition twice with 2 different keywords.

Few issues: padding chars?

(1) Use none + some columns are different length

(2) Use them, and you might have to pad twice!

9/12/16 (3)

(5) (1) (7) (2) (6) (3) (4)

Keyword: HARAMBE

THESECO
NDHOMEW
ORKASSI
GNMENTI
SDUESOO
NGOODLU
CK

Cipher

HDRNDGKSOAEEOCESTOL

OWIIOUTNOGSNCEMSNSD

EHKMUO

44 chars

9/12/16 (4)

5	1	7	2	6	3	4
T	H	E	S	E	C	O
N	D	H	O	M	E	W
O	R	K	A	S	S	I
G	N	M	E	N	T	I
S	D	U	E	S	O	O
W	G	O	O	D	L	U
C	K					

Rules: Write down keyword, number columns, accordingly

Calculate x = (msg len) / (# columns)

Calculate y = (msg len) % (# columns

→ length of "short" columns

→ number of columns w/ extra letter

Read ciphertext in order, placing letters in the column numbered 1, then 2, etc. When placing letters determine the # of letters to place. Place x letters in short columns and x+1 letters in long columns. The long columns are the first y columns from the left. In this case, the columns numbered 5 and 1, respectively.

Hill cipher cryptanalysis with matching plain/cipher pair.

K HOME

$$\begin{bmatrix} 3 & 2 \\ 10 & 7 \end{bmatrix}\begin{bmatrix} 7 \\ 14 \end{bmatrix} = \begin{bmatrix} 3\times 7+2\times 14 \\ 10\times 7+7\times 14 \end{bmatrix} \quad \text{mod } 26$$

$$= \begin{bmatrix} 21+28 \\ 20+98 \end{bmatrix} = \begin{bmatrix} 49 \\ 118 \end{bmatrix} = \begin{matrix} 23 \\ 12 \end{matrix}$$

$$\begin{array}{r} 168 \\ -156 \\ \hline 12 \end{array}$$

HO → XM
(7,14) → (23,12)

$$\begin{bmatrix} 3 & 2 \\ 10 & 7 \end{bmatrix}\begin{bmatrix} 12 \\ 4 \end{bmatrix} = \begin{bmatrix} 3\times 12+2\times 4 \\ 10\times 12+7\times 4 \end{bmatrix}$$

$$= \begin{bmatrix} 36+8 \\ 120+28 \end{bmatrix}$$

$$= \begin{bmatrix} 44 \\ 148 \end{bmatrix} = \begin{bmatrix} 18 \\ 18 \end{bmatrix} \text{ mod } 26$$

(ME) → SS
(12,4) → (18,18)

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} 18 \\ 18 \end{bmatrix} = \begin{bmatrix} 18a+18b \\ 18c+18d \end{bmatrix} = \begin{bmatrix} 12 \\ 4 \end{bmatrix}$$

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} 23 \\ 12 \end{bmatrix} = \begin{bmatrix} 23a+12b \\ 23c+12d \end{bmatrix} = \begin{bmatrix} 7 \\ 14 \end{bmatrix}$$

9/16/16

$$18a + 18b = 12 \mod 26$$
$$23a + 12b = 7 \mod 26$$

$$-\quad 36a + 36b = 24 \mod 26$$
$$69a + 36b = 21 \mod 26$$

$$33a = -3 \mod 26$$
$$15(7a) \equiv 15(-3) \mod 26$$
$$a \equiv -45 \mod 26$$
$$a \equiv 7 \mod 26$$

$$18(7) + 18b \equiv 12 \mod 26$$
$$126 + 18b = 12 \mod 26$$
$$18b \equiv -114 \mod 26$$ (Note $-114 \equiv 16 \mod 26$)

$$18b = 26c + 16$$
$$9b = 13c + 8$$
$$3(9b) \equiv 3(8) \mod 13$$
$$b \equiv 24 \mod 13$$
$$\equiv 11 \mod 13$$

$a = 7$ $\quad$ $b = 11$ or 24