Rectangular Transposition

Plaintext:

Why did you bring that book that I didn't want to be read to out of from up for?

Key: 6 1 2 4 5 3

6	1	2	4	5	3
W	H	Y	D	I	D
Y	O	U	B	R	I
N	G	T	H	A	T
B	O	O	K	T	H
A	T	I	D	I	D
N	T	W	A	N	T
T	O	B	E	R	E
A	D	T	O	O	U
T	O	F	F	R	O
M	U	P	F	O	R

A word may also be used as a key because it is easier to remember. We will use the convention that the word is turned into a permutation by placing a number below each letter corresponding to its alphabetical order.

Examples:

ATOM CONDOR HAMBURGER

Rectangular Transposition

Plaintext:

Why did you bring that book that I didn't want to be read to out of from up for?

Key: 6 1 2 4 5 3

6	1	2	4	5	3
W	H	Y	D	I	D
Y	O	U	B	R	I
N	G	T	H	A	T
B	O	O	K	T	H
A	T	I	D	I	D
N	T	W	A	N	T
T	O	B	E	R	E
A	D	T	O	O	U
T	O	F	F	R	O
M	U	P	F	O	R

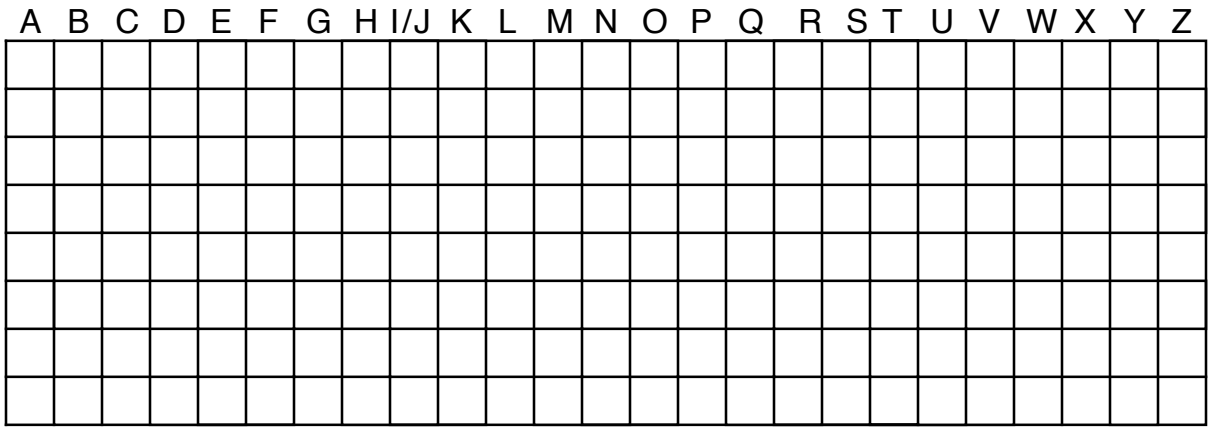
HOGOT TODOU YUTOI WBTFP DITHD TEUOR DBHKD AEOFF
IRATI NRORO WYNBA NTATM

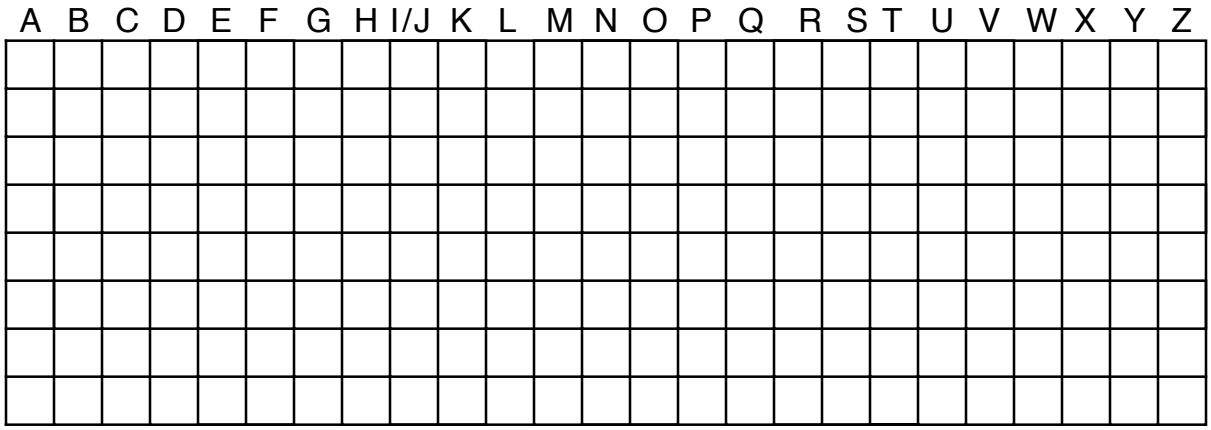
A word may also be used as a key because it is easier to remember. We will use the convention that the word is turned into a permutation by placing a number below each letter corresponding to its alphabetical order.

Examples:

ATOM	CONDOR	HAMBURGER
1432	143256	516297438

Homophonic Substitution





Homophonic Substitution

	A	B	C	D	E	F	G	H	I/J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
S	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	1	2	3	4	5	6	7	8
T	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	1	2	3	4	5	6	7
A	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
N	14	15	16	17	18	19	20	21	22	23	24	25	1	2	3	4	5	6	7	8	9	10	11	12	13

A	B	C	D	E	F	G	H	I/J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	1	2	3	4	5	6	7	8
33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	26	27	28	29	30	31	32
51	52	53	54	55	56	57	58	59	60	61	62	63	64	65	66	67	68	69	70	71	72	73	74	75
89	90	91	92	93	94	95	96	97	98	99	100	76	77	78	79	80	81	82	83	84	85	86	87	88

Key: STAN

Plaintext #1: T H E N W H Y D I D Y O U T

U R N S O M E O F U S I N S

I D E O U T ?

Cyphertext #2: 69-16-9-2-85-33-81-35-51-25-61-40-13-1-45-93-85-20-64-77

ADFGVX

The ADFGVX system was first used in the battlefield
march 5th 1918. Was broken June 1st by Georges Painvin

K1: A 6x6 square K2: a permutation of n (n even)

C	O	8	X	F	4
M	K	3	A	Z	9
N	W	L	0	J	D
5	S	I	Y	H	U
P	1	V	B	6	R
E	Q	7	T	2	G

4	9	5	15	2	8	16	12	13	17	1	18	3	19	10	7	6	11	14	20
H		Q		R		E		Q		U		E		S		T		S	
F		R		O		N		T		L		I		N		E		S	
I		T		U		A		T		I		O		N		B		Y	
T		E		L		E		G		R		A		M		H		Q	
7		T		H		C		O		R		P		S		E		D	

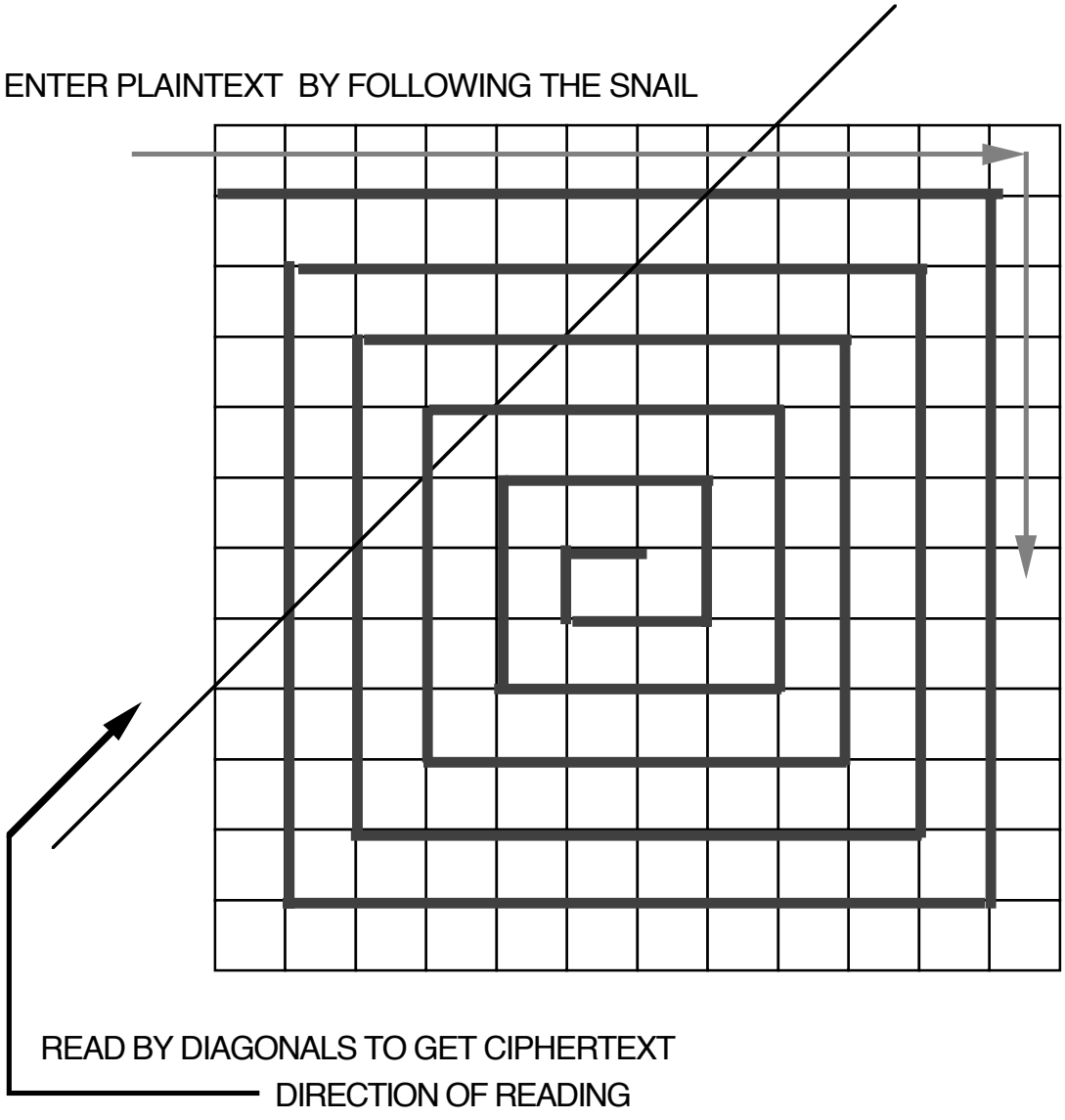
GFGVV VAGFG XGADV GAGXX XVXXX XXVGX

DAAAD XDXFV VVFGF GFFDG GAGVA AAGAA

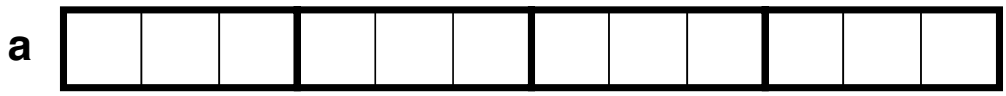
XXXVA GGGXF DXGAG XFDXA DGGVD XFFXF

AFDGA DDGDX

THE SNAIL ENCRYPTION SYSTEM



VERNAM TWO-TAPE SYSTEM



A	0	H	7	N	13	U	20
B	1	I	8	O	14	V	21
C	2	J	9	P	15	W	22
D	3	K	10	Q	16	X	23
E	4	L	11	R	17	Y	24
F	5	M	12	S	18	Z	25
G	6			T	19		

THE VERNAM CIPHER

THEOREM

$a_1\ a_2\ a_3 \ldots a_n \ldots$ periodic of period p

$$a_{n+p} = a_n$$

$b_1\ b_2\ b_3 \ldots b_n \ldots$ periodic of period q

$$b_{n+q} = b_n$$

$$r_n = a_n + b_n$$

periodic of period $\dfrac{p \times q}{(p,q)}$

(p,q) = gcd p & q

EXAMPLE

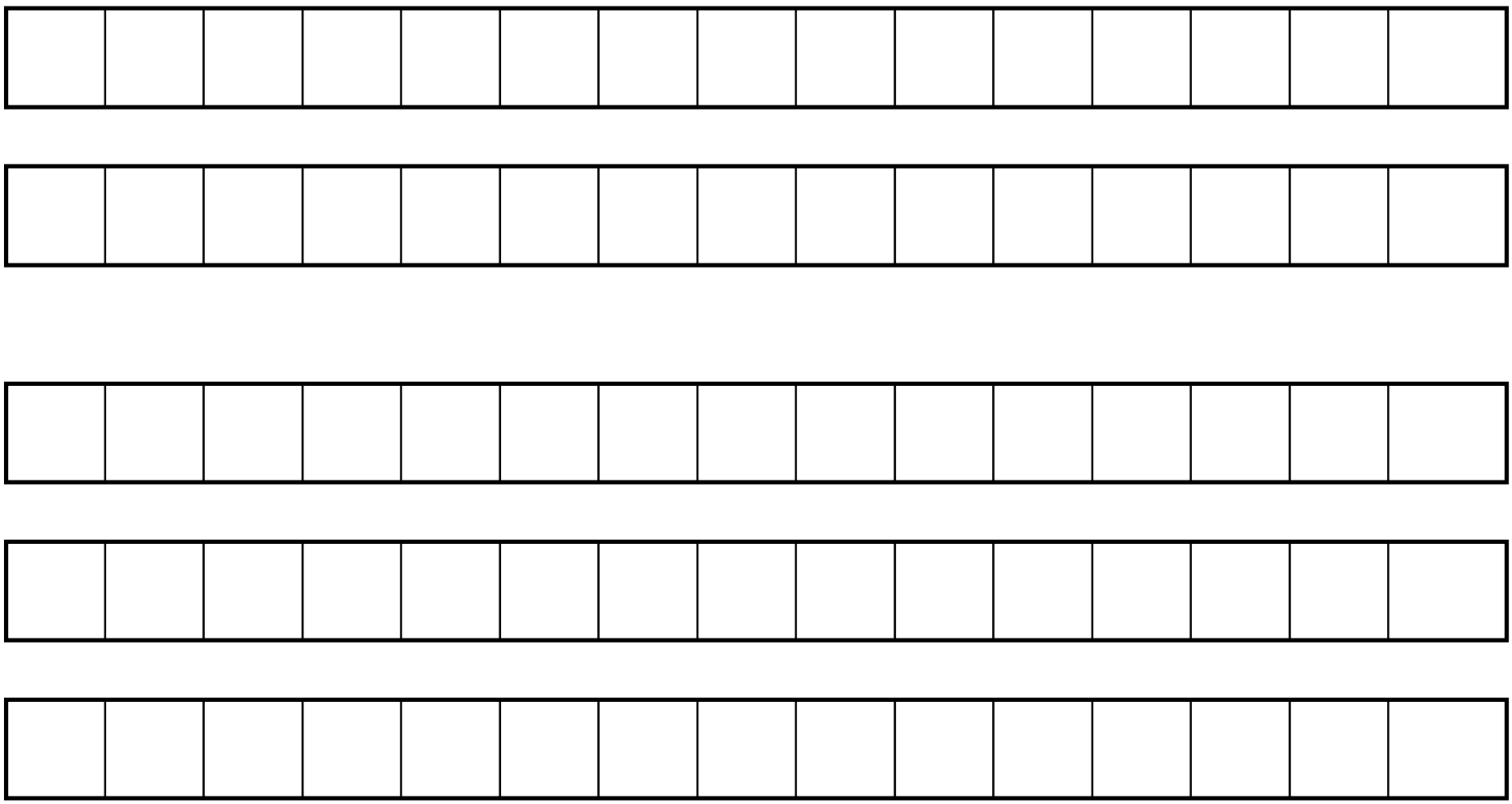
$p = 100$ $b = 101$ $(p,q) = 1$ period $r = 10{,}101$.

Fact: If a and b are chosen at random then r

has no smaller period than $\dfrac{p \times q}{(p,q)}$

p=3 q=5

a1	a2	a3	a1	a2	a3	a1	a2	a3	a1	a2	a3	a1	a2	a3	a1	a2
b1	b2	b3	b4	b5	b1	b2	b3	b4	b5	b1	b2	b3	b4	b5	b1	b2
r1	r2	r3	r4	r5	r6	r7	r8	r9	r10	r11	r12	r13	r14	r15	r1	r2



A 0	F 5	K 10	P 15	U 20
B 1	G 6	L 11	Q 16	V 21
C 2	H 7	M 12	R 17	W 22
D 3	I 8	N 13	S 18	X 23
E 4	J 9	O 14	T 19	Y 24

Z 25

Hill Encipherment

A	0
B	1
C	2
D	3
E	4
F	5
G	6
H	7
I	8
J	9
K	10
L	11
M	12
N	13
O	14
P	15
Q	16
R	17
S	18
T	19
U	20
V	21
W	22
X	23
Y	24
Z	25

Key: a kxk matrix

ALL ARITHMETIC IS DONE (MOD 26)

$$A = \begin{bmatrix} 11 & 2 \\ 1 & 5 \end{bmatrix} \quad k=2 \qquad A^{-1} = \begin{bmatrix} 5 & -2 \\ -1 & 11 \end{bmatrix} = \begin{bmatrix} 5 & 24 \\ 25 & 11 \end{bmatrix}$$

$$\det A = 11*5 - 2*1 = 53 \equiv 1 \pmod{26}$$

$$\begin{bmatrix} 11 & 2 \\ 1 & 5 \end{bmatrix}\begin{bmatrix} 5 & 24 \\ 25 & 11 \end{bmatrix} = \begin{bmatrix} 55+50 & 264+22 \\ 5+125 & 24+55 \end{bmatrix}$$

Plaintext: MEAT

Numerical: 12-4 0-19

A*plaintext:

Cyphertext:

Cyphertext: WU UO EI AY

Numerical: 22-20 20-14 4-8 0-24

A^{-1}*Cyphertext:

Plaintext:

Playfair Cipher

Key:

D	E	N	I	A
L	B	C	F	G
H	K	M	O	P
Q	R	S	T	U
V	W	X	Y	Z

Plaintext:

382 Robertson Dr, West Hollywood

TH RE EQ EI GH TQ TW OR OB ER TS ON

DR WE ST HO LQ LY WO OD