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

Start with 1

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	← 1-25
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	← 26-50
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	← 51-75
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	← 76-100

Key: STAN

Plaintext #1: T H E N W H Y D I D Y O U T
82-16-55-45
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
THATWASCARLHESNEWMOO

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)

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

← first key

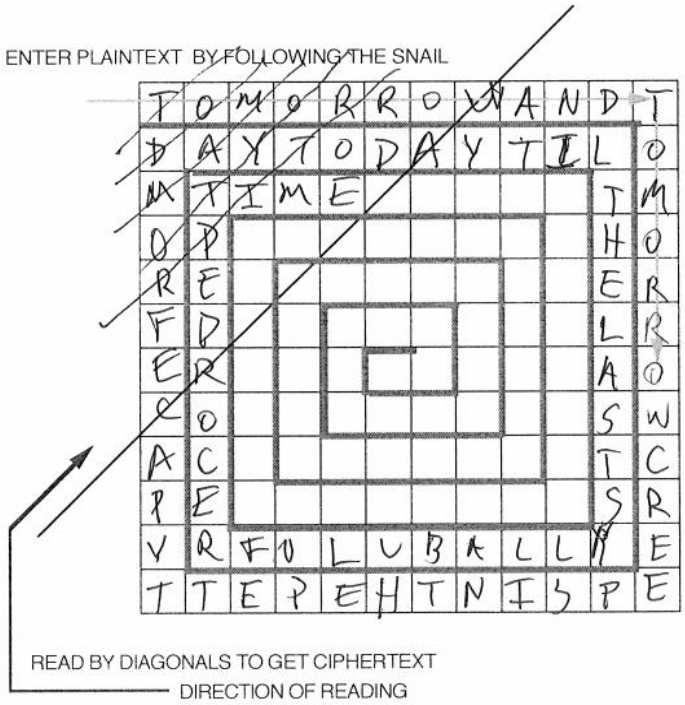
4	9	5	15	2	8	16	12	13	17	1	18	3	19	10	7	6	11	14	20
G	V	X	D	V	X	X	A	X	D	G	X	X	A						
H	Q	R	E	Q	U	E		S		T		S							
A	V	V	X	A	D	F	A	X	G	F	F	G	F						
F	R	O	N	T	L	I		N		E		S							
G	F	X	G	G	X	D	G	X	G	G	F	A	D						
I	T	U	A	T	I	O		N		B		Y							
X	G	X	A	F	F	X	A	X	X	V	X	D	G						
T	E	L	E	G	R	A		M		H		Q	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

← second Key

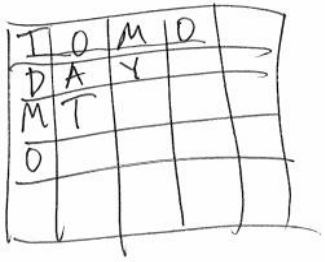
GFGVV VAGFG XGADV GAGXX XVXXX XXVGX
DAAAD XDXFV VVFGF GFFDG GAGVA AAGAA
XXXVA GGGXF DXGAG XFDXA DGGVD XFFXF
AFDGA DDGDX

← encrypted message

THE SNAIL ENCRYPTION SYSTEM



TDOMAM OTYO RPITR...



p=3 q=4 a key OUT

VERNAM TWO-TAPE SYSTEM

	O	U	T	O	U	T	O	U	T	O	U	T	O U T C
a	14	20	19	14	20	19	14	20	19	14	20	19	
	D	R	O	P	D	R	O	P	D	R	O	P	PRO P
b	3	17	14	15	3	17	14	15	3	17	14	15	
r	17	11	7	3	23	10	2	19	22	5	8	8	

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		

plaintext	
numerical	
r	
numerical	
ciphertext	

Hill Encipherment

Key: a kxk matrix

ALL ARITHMETIC IS DONE (MOD 26)

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

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

$1 \cdot (11 \cdot 5 - 2 \cdot 1) \equiv 1 \pmod{26}$

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

A^{-1}

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

Plaintext: MEAT

Numerical: 12-4 0-19

A*plaintext: $\begin{bmatrix} 11 & 2 \\ 1 & 5 \end{bmatrix}\begin{bmatrix} 12 \\ 4 \end{bmatrix}$ $\begin{bmatrix} 11 & 2 \\ 1 & 5 \end{bmatrix}\begin{bmatrix} 0 \\ 19 \end{bmatrix}$

95-78
17

Cyphertext: $11 \cdot 12 + 2 \cdot 4$ $12 \cdot 1 + 4 \cdot 5$ $2 \cdot 19$ $5 \cdot 19$

10 6 12 17 → KGMR

Cyphertext: WU UO EI AY

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

A^{-1}*Cyphertext: $\begin{bmatrix} 5 & -2 \\ -1 & 11 \end{bmatrix}\begin{bmatrix} 22 & 20 & 4 & 0 \\ 20 & 14 & 8 & 24 \end{bmatrix}$

Plaintext: $5 \cdot 22 - 2 \cdot 20$ $-1 \cdot 22 + 11 \cdot 20$ $5 \cdot 20 - 2 \cdot 14$

18 16 20

S Q U

$A^{-1} \cdot A = I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$

$-1 \cdot 20 + 11 \cdot 14$ $5 \cdot 4 - 2 \cdot 8$ $-1 \cdot 4 + 11 \cdot 8$ $-2 \cdot 24$ $11 \cdot 24$

4 4 6 4 4

E E G E E

$A^{-1} \cdot$ cyphertext

$\equiv A^{-1} \cdot A *$ plaintext

$\equiv I *$ plaintext

$\equiv$ plaintext

220
− 22
198

84

$26 \overline{)198}$ 7, 182, 16

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
QO WB DR NA LP VR RY KT KF BW UT MI
DR WE ST HO LQ LY WO OD
~~QE~~ EB TV KP HV FV YK HI
EQ

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

$$A^{-1} = \begin{bmatrix} d & -b \\ -c & a \end{bmatrix} \cdot \frac{1}{ad-bc}$$

$$A^{-1} \cdot A = \begin{bmatrix} \frac{d}{ad-bc} & \frac{-b}{ad-bc} \\ \frac{-c}{ad-bc} & \frac{a}{ad-bc} \end{bmatrix} \cdot \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

$$= \begin{bmatrix} \frac{ad-bc}{ad-bc} & \frac{bd-bd}{ad-bc} \\ \frac{-ac+ac}{ad-bc} & \frac{-bc+ad}{ad-bc} \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

Mod 26

Find e s.t.

$$(ad-bc) \cdot e \equiv 1 \pmod{26}$$

$$e \equiv (ad-bc)^{-1} \pmod{26}$$

And

$$A^{-1} \equiv \begin{bmatrix} d & -b \\ -c & a \end{bmatrix} \cdot e \pmod{26}$$

then

$$A^{-1} \cdot A \equiv \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \pmod{26}$$

Sometimes

det A will have a common factor with the modulus 26.

if it does then there will not be a value e s.t.

$$e \cdot \det A \equiv 1 \pmod{26}$$

the inverse of A does not exist

By working mod 29, in this case

then det A only has a common factor with 29 if it is a multiple of 29.

A → 0
B → 1
C → 2
⋮
Z → 25

Ø → 26
1 → 27
2 → 28

← choose a convention that the last 3 symbols go to 26, 27, 28

If A doesn't have an inverse the plaintext may not be recoverable from the cyphertext.