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

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	G	D	X	G	G	D
H		Q		R		E		Q		U		E		S		T		S	
A	Y	V	X	A	D			X	G	F	F					X	A	G	D
F		R		O		N		T		L		I		N		E		S	
				G	X			X	G	G	F								
I		T		U		A		T		I		O		N		B		Y	
				F	F	x	A	X	X	V	X					G	V	X	D
T		E		L		E		G		R		A		M		H		Q	
				G	V					V	X			G	D	X	A		
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

Formula for the inverse of a Matrix

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \qquad A^{-1} = \cancel{\begin{bmatrix} d & c \\ -b & d \end{bmatrix}(ad-bc)^{-1}}$$

$$\begin{bmatrix} d & -b \\ -c & a \end{bmatrix}(ad-bc)^{-1}$$

$a \equiv b \pmod{n}$

$a-b$ is divisible by n

OR $a-b$ is a multiple of n

OR $a-b = n \cdot k$ for some k

OR n divides $a-b$

if $a=b$ then $a \equiv b \pmod{n}$

if $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$
then $a \equiv c \pmod{n}$

if $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$
then $ac \equiv bd \pmod{n}$
and $a+c \equiv b+d \pmod{n}$

If n is relatively prime to a (no common factors)
then $\exists b$ s.t. $a \cdot b \equiv 1 \pmod{n}$

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)

k=2

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

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

$$\begin{bmatrix} 11 & 2 \\ 1 & 5 \end{bmatrix}\begin{bmatrix} 5 & 24 \\ 25 & 11 \end{bmatrix} = \begin{bmatrix} \overset{\equiv 1 \,(\mathrm{mod}\ 26)}{55+50} & \overset{\equiv 0 \,(\mathrm{mod}\ 26)}{\underset{= 26 \cdot 11}{264+22}} \\ \underset{\substack{= 5 \cdot 26 \\ \equiv 0 \,(\mathrm{mod}\ 26)}}{5+125} & \underset{\equiv 1 \,(\mathrm{mod}\ 26)}{24+55} \end{bmatrix}$$

Encryption

Plaintext: MEAT

Numerical: 12-4 0-19

A*plaintext: 10-6 12-17

Cyphertext: KG MR

A · plaintext

$$\begin{bmatrix} 11 & 2 \\ 1 & 5 \end{bmatrix}\begin{bmatrix} 12 & 0 & \cdots \\ 4 & 19 & \end{bmatrix} = \begin{bmatrix} 2+8 & 12 \\ 6 & 17 \end{bmatrix}$$

Cyphertext: WU UO EI AY

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

A^{-1}*Cyphertext: 18-16 20-4 4-6 4-4

Plaintext: SQ UE EG EE

$$\overset{A^{-1}}{\begin{bmatrix} 5 & 24 \\ 25 & 11 \end{bmatrix}}\begin{bmatrix} 22 & 20 & 4 & 0 \\ 20 & 14 & 8 & 24 \end{bmatrix}$$

$$\begin{bmatrix} 18 & 20 & 4 & 4 \\ 16 & 4 & 6 & 4 \end{bmatrix} = \begin{bmatrix} 6+12 & 22+24 & 20+10 & 0+4 \\ 4+12 & 6+24 & 22+10 & 0+4 \end{bmatrix}$$

VERNAM TWO-TAPE SYSTEM

a	12	14	7	12	14	7	12	14	7	12	14	7
b	8	2	16	23	8	2	16	23	8	2	16	23
r	20	16	23	9	22	9	2	11	15	14	4	4

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

plaintext												
numerical												
r												
numerical												
ciphertext												

ULD PCJQADEDW NDQUJEVCD ULJU
THE BLACKENED RECTANGLE THAT

GJB OHCCDW RHU RK ULD URJBUDN
WAS PULLED OUT O THE TOASTER
F

XTVLU REQD LJYD PDDE J
MIGHT ONCE HAVE BEEN A

ORO-UJNU.
POP TART

Characters: 74

Guess at a few letters.
1) Look for common letters at the beginning of words, and for short words. "THE" and "AND" are common three letter words. The only 1 letter words are "A" and "I".
2) Look at contextual clues such as punctuation and spacing. (e.g. If there is and apostrophe, it is usually quite easy to guess at the letter immediately following).
3) Use general knowledge about English
4) ETOANIRSH
5) common beginnings and endings of words (e.g. -ING).