DESIGN CONSIDERATIONS OF A CIPHER

There are ways of sending data so that is theoretically impossible to recover the message without knowing the key. Systems like this are rarely used because they are inconvenient. The key may only be used once and must be as long as the message that is being sent.

- Type of data (TV signal/voice/computer data/letter/telegram)
- Security
- Ease of Use
- Cost/ease of use vs. value of data
- Amount of data
- training of the people who do the encryption is simple (because they die frequently)

Zimmermann Telegram

From Wikipedia, the free encyclopedia

The **Zimmermann Telegram** (or **Zimmermann Note**; German: *Zimmermann-Depesche*; Spanish: *Telegrama Zimmermann*) was a coded telegram dispatched by the Foreign Secretary of the German Empire, Arthur Zimmermann, on January 16, 1917, to the German ambassador in Mexico, Heinrich von Eckardt, at the height of World War I.

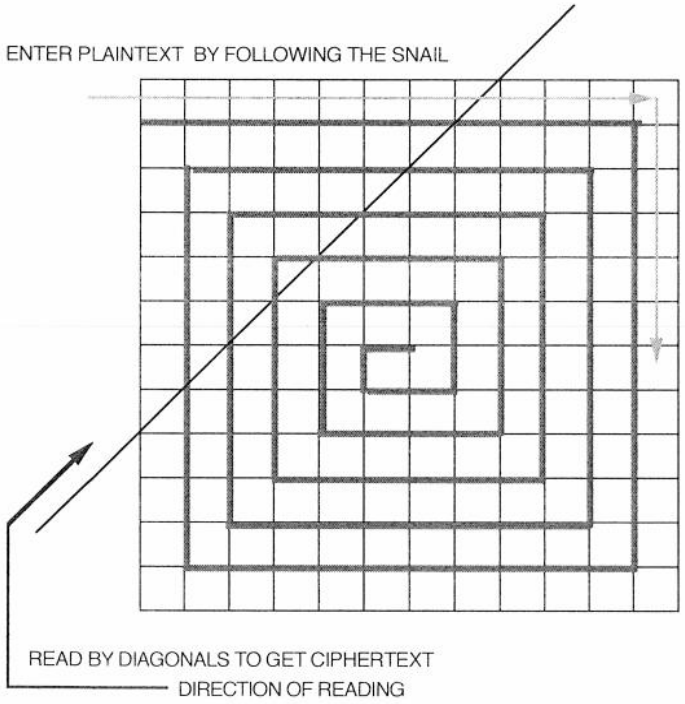
The telegram instructed the ambassador to approach the Mexican government with a proposal to form a military alliance against the United States. It promised Mexico land in the United States if they were to help. It was intercepted and decoded by the British, and its contents hastened the entry of the United States into World War I.

The Zimmermann telegram as it was sent from Washington to Mexico

username:
416user
password:
purple

garsia.math.yorku.ca/~zabrocki/math416/w12/

THE SNAIL ENCRYPTION SYSTEM



p=3 q=4 a key OUT

VERNAM TWO-TAPE SYSTEM

	O	U	T	O	U	T	O	U	T	O	U	T	OUT OUT
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	DRO PDR
b	3	17	14	15	3	17	14	15	3	17	14	15	
r	17	11	7	3	23	10	2	9	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)

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

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

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

A	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:

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

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

The Vigenere Square

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

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		

Caesar Cipher

plaintext	B	R	E	A	T	H	O	F	F	R	E	S
numerical	1	17	4	0	19	7	14	5	5	17	4	18
plaintext+key (mod 26)	4	20	7	3	22	10	17	8	8	20	7	21
ciphertext	E	V	H	D	W	K	R	I	I	U	H	V

Vigenere Cipher

plaintext	B	R	E	A	T	H	O	F	F	R	E	S
numerical	1	17	4	0	19	7	14	5	5	17	4	18
key	Q	U	I	K	Q	U	I	K	Q	U	I	K
plaintext + key (mod 26)	17	11	12	10	9	1	22	15	21	11	12	2
ciphertext	R	L	M	K	J	B	W	P	V	L	M	C

6x4 X

12x2

3x8

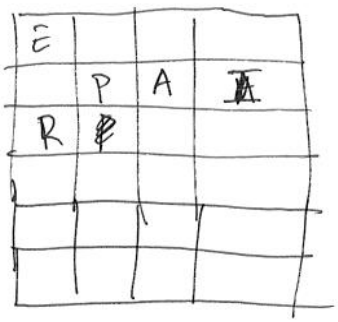
4x6

8x3

2x12

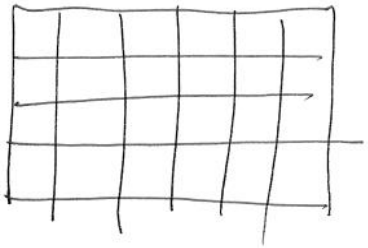
24x1

1x24



~~masere~~

N W E N
A E P I
S O R V
E E D A
R N L S
E O Y N



N R O E L V
A E E P Y A
S W N R N S
E E O D I N

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)

	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	[illegible]	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

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

3 5	1 7	9 4	10 2	8 6
A V	A D			
E	L			
A D	F F			
L	I			