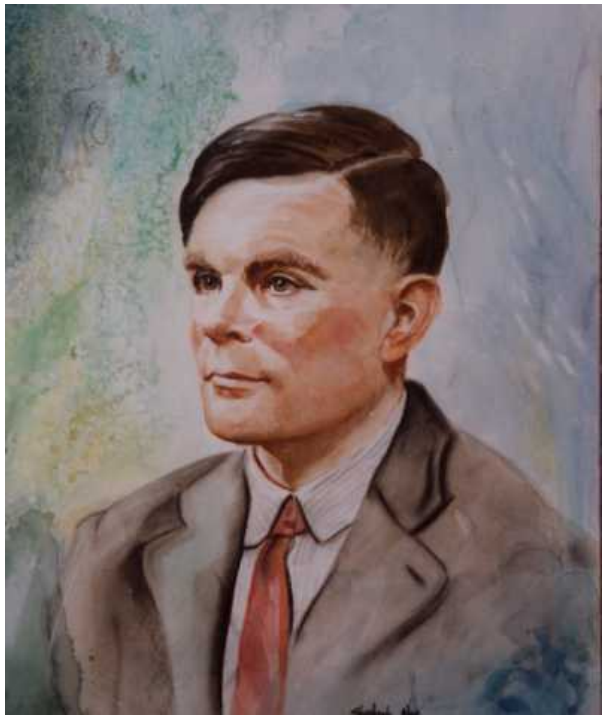
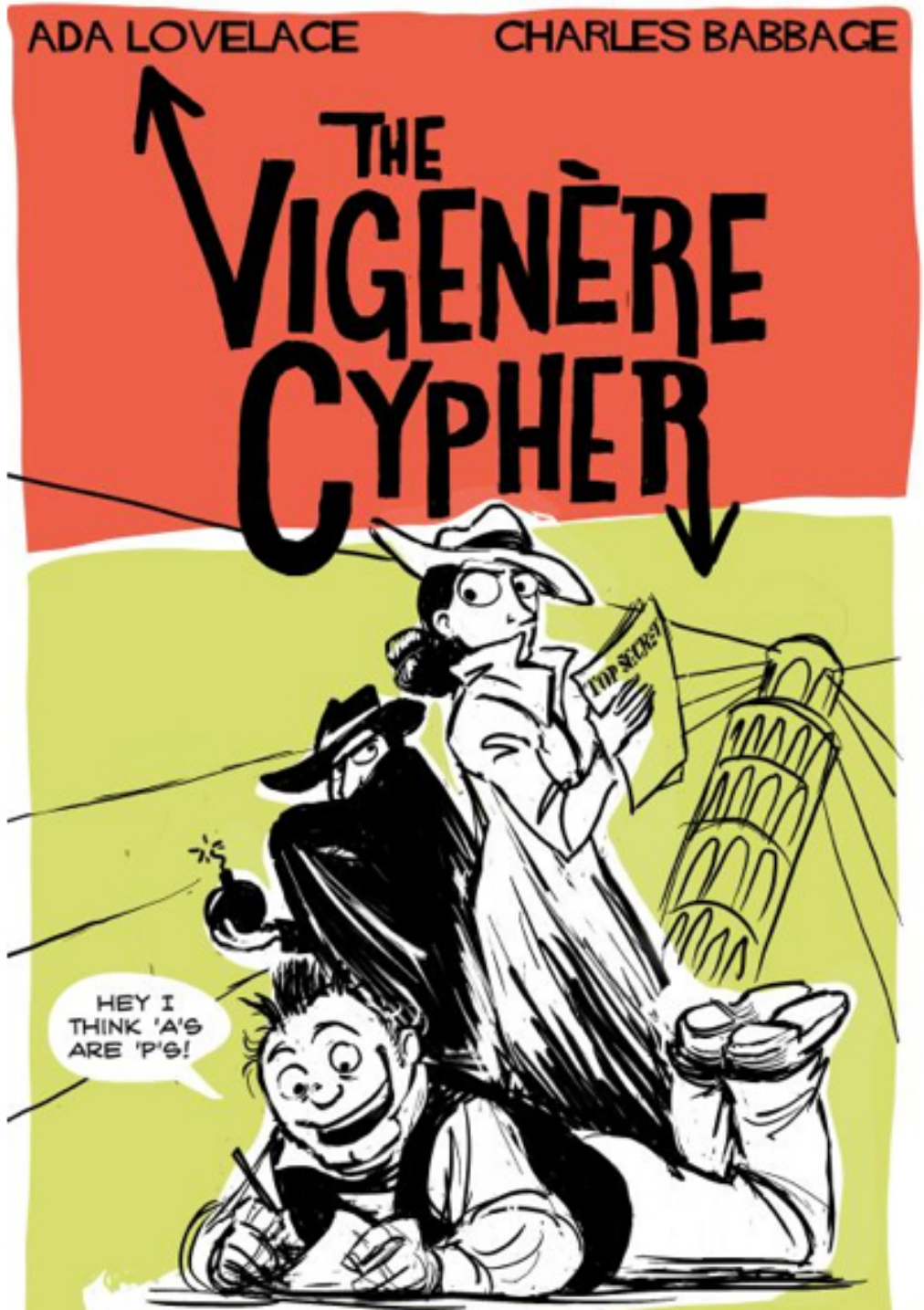


Code Makers and Code Breakers From Julius Caesar To Alan Turing And Beyond V

An Introduction To Some Mathematics and Linguistics Used to Crack Secret Ciphers


ADA LOVELACE
CHARLES BABBAGE
THE VIGENÈRE CYPHER
TOP SECRET
HEY I THINK 'A'S ARE 'P'S!

Detecting a Polyalphabetic Cipher

A monoalphabetic cipher has greater variation among frequencies of the individual letters

William Friedman (1930)

Index of Coincidence

Index of Coincidence

$$\sum_{i=A}^{Z} \frac{f_i(f_i - 1)}{N(N-1)}$$

f_i = frequency of letter i
N = number of characters in message

Number of Alphabets	Expected IC
1	.066
2	.052
5	.044
10	.041
26	.038

The Vigenère Cipher Was Secure for 300 Years

The Vigenère Cipher Was Secure for 300 Years

A Simple Mathematical Idea Destroyed Its Apparent Security

The Vigenère Cipher Was Secure for 300 Years

A Simple Mathematical Idea Destroyed Its Apparent Security

If the keyword has n letters and some word appears in the plaintext more than n times, then that word will be enciphered the same way at least twice in the cipher text.

How Can We Make a Vigenère Cipher More Secure?

How Can We Make a Vigenère Cipher More Secure? Try To Get Rid of Repetitions

How Can We Make a Vigenère Cipher More Secure?
Try To Get Rid of Repetitions
How?

How Can We Make a Vigenère Cipher More Secure?

Try To Get Rid of Repetitions

How?

Make Keyword Longer

How Can We Make a Vigenère Cipher More Secure?

Try To Get Rid of Repetitions

How?

Make Keyword Longer

Take Keywords Longer Than Length of Plaintext

Take Keywords Longer Than Length of Plaintext

Examples

Declaration Of Independence
The Bible

Try This At Home:

1. Take two long texts (2000 or more characters in length)

Try This At Home:

1. Take two long texts (2000 or more characters in length)
2. Choose one of them for the Keyword and the other for the Plaintext

Try This At Home:

1. Take two long texts (2000 or more characters in length)
2. Choose one of them for the Keyword and the other for the Plaintext
3. Use our Vigenère program to generate the ciphertext

Try This At Home:

1. Take two long texts (2000 or more characters in length)
2. Choose one of them for the Keyword and the other for the Plaintext
3. Use our Vigenère program to generate the ciphertext
4. How flat is the frequency count for the cipher text?

Try This At Home:

1. Take two long texts (2000 or more characters in length)
2. Choose one of them for the Keyword and the other for the Plaintext
3. Use our Vigenère program to generate the ciphertext
4. How flat is the frequency count for the cipher text?
5. What is the longest string in the cipher text that repeats itself?

Possible Weaknesses of This Approach

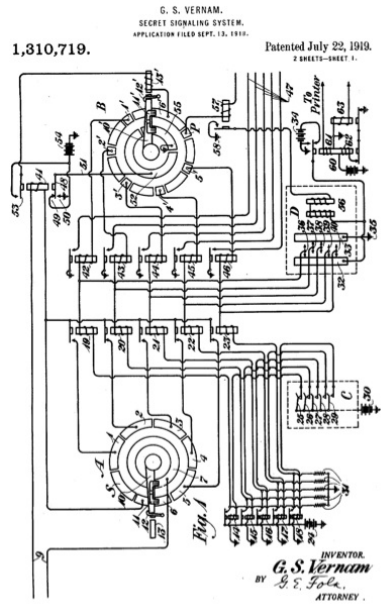
IS THERE A THEORETICALLY UNBREAKABLE CIPHER SCHEME?

IS THERE A THEORETICALLY UNBREAKABLE CIPHER SCHEME?

THE ONE TIME PAD

Each character in plaintext is shifted by a random number

Gilbert Vernam
1890 – 1960



Vernam's Patent Figure

USING A ONE TIME PAD

11	25	20	14	13	12	9	18	21	5	24	17	18	9	5
12	8	2	1	12	9	14	13	15	23	17	9	21	14	17
20	15	24	5	17	21	10	21	5	5	26	3	22	22	23
1	4	14	18	24	2	18	4	17	18	21	22	10	5	21
1	13	2	8	26	2	5	1	3	25	2	2	12	19	21
4	4	21	8	12	11	7	17	18	14	20	18	18	19	12
2	22	20	14	10	20	4	13	23	13	5	1	5	6	14
14	16	3	8	16	9	9	14	14	21	3	17	25	24	15
26	23	12	19	23	3	8	4	17	23	17	6	24	20	16
17	4	10	15	16	26	14	3	2	22	10	1	22	23	17
13	18	25	24	10	17	14	12	26	23	15	7	5	26	19
21	21	3	16	16	20	9	21	12	23	16	21	1	6	10

M	A	T	H	E	M	A	T	I	C	S
13	1	20	8	5	13	1	20	9	3	19
11	25	20	14	13	12	9	18	21	5	24
24	26	40	22	18	25	10	38	30	8	43
24	26	14	22	18	25	10	12	4	8	17
X	Z	N	V	R	Y	J	L	D	H	Q

Vernam One Time Pad in Binary

Add Modulo 2 with no carries; Also called XORing

$$0 + 0 = 0$$
$$0 + 1 = 1$$
$$1 + 0 = 1$$
$$1 + 1 = 0$$

Letter	Position	Binary
A	1	00001
B	2	00010
C	3	00011
D	4	00100
E	5	00101
F	6	00110
G	7	00111
H	8	01000
I	9	01001
J	10	01010
K	11	01011
L	12	01100
M	13	01101
N	14	01110
O	15	01111
P	16	10000

Letter	Position	Binary
Q	17	10001
R	18	10010
S	19	10011
T	20	10100
U	21	10101
V	22	10110
W	23	10111
X	24	11000
Y	25	11001
Z	26	11010
[SPACE]	27	11011
.	28	11100
,	29	11101
!	30	11110
:	31	11111
;	32	00000

plaintext: THIS IS THE MESSAGE

One Time Pad: 01010100100100011110001111000011?

0	1	0	1	0	1	0	0	1	0	0	1	0	0	0
1	0	1	0	0	0	1	0	0	0	0	1	0	0	1
1	1	1	1	0	1	1	0	1	0	0	0	0	0	1

Letter	Position	Binary
A	1	00001
B	2	00010
C	3	00011
D	4	00100
E	5	00101
F	6	00110
G	7	00111
H	8	01000
I	9	01001
J	10	01010
K	11	01011
L	12	01100
M	13	01101
N	14	01110
O	15	01111
P	16	10000

Letter	Position	Binary
Q	17	10001
R	18	10010
S	19	10011
T	20	10100
U	21	10101
V	22	10110
W	23	10111
X	24	11000
Y	25	11001
Z	26	11010
[SPACE]	27	11011
.	28	11100
,	29	11101
!	30	11110
:	31	11111
;	32	00000

0	1	0	1	0	1	0	0	1	0	0	1	0	0	0
1	0	1	0	0	0	1	0	0	0	0	1	0	0	1
1	1	1	1	0	1	1	0	1	0	0	0	0	0	1

11110 becomes !

11010 becomes Z

00001 becomes A

Ciphertext begins **!ZA**

Thoughts About The One–Time Pad

Thoughts About The One–Time Pad
In Theory: Completely Secure

Thoughts About The One–Time Pad

In Theory: Completely Secure

Practical Problems:

Thoughts About The One–Time Pad
In Theory: Completely Secure
Practical Problems:

- Pad must be randomly generated.

Thoughts About The One–Time Pad
In Theory: Completely Secure
Practical Problems:

- Pad must be randomly generated.
- You and your friend need identical pads.

Thoughts About The One–Time Pad
In Theory: Completely Secure
Practical Problems:

- Pad must be randomly generated.
- You and your friend need identical pads.
- You must stay synchronized.

Thoughts About The One–Time Pad

In Theory: Completely Secure

Practical Problems:

- Pad must be randomly generated.
- You and your friend need identical pads.
- You must stay synchronized.
- You must use the pad only once.

Thoughts About The One–Time Pad
In Theory: Completely Secure
Practical Problems:

- Pad must be randomly generated.
- You and your friend need identical pads.
- You must stay synchronized.
- You must use the pad only once.
- Creation, Distribution, and Storage of pads are a problem.

Thoughts About The One–Time Pad
In Theory: Completely Secure
Practical Problems:

- Pad must be randomly generated.
- You and your friend need identical pads.
- You must stay synchronized.
- You must use the pad only once.
- Creation, Distribution, and Storage of pads are a problem.
- How many pads would the State Department require?

THE

MACHINE


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


Zur Beachtung!
Nur Glühlampen mit 12 mm Durchmesser verwenden.
Q W E R T Z U I O
A S D F G H J K
P Y X C V B N M L
Klappe schliessen
ENIGMA

Think of the Enigma Machine as a Vigenère Cipher With a Keyword of Length

$$26 \times 26 \times 26 = 17,576$$