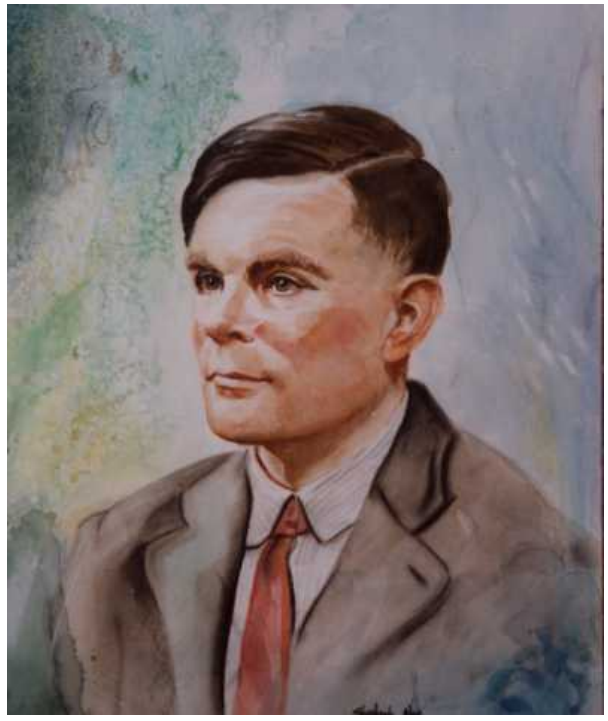

Code Makers and Code Breakers From Julius Caesar To Alan Turing And Beyond VI

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

Tonight

Decoding Nazi Secrets Transcript of Film *Some People in Film*

Enigma in Action

Sekret Enigmy (*Enigma Secret*)

Wednesday

https://enigmamuseum.com

Tom Perera

Dan Perera

Friday

Fall Family Weekend

Parents Invited

Class Will Meet in Warner 101

Tonight

Decoding Nazi Secrets Transcript of Film *Some People in Film*

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**

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 Vigenè Cipher
With a Keyword of Length

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