



Code Makers and Code Breakers
From Julius Caesar To Alan Turing
And Beyond II:
An Introduction To
Some Mathematics and Linguistics
Used to Crack Secret Ciphers



Caesar Cipher: Replace each letter of the message by the letter 3 places beyond it in the normal alphabet

Caesar Cipher: Replace each letter of the message by the letter 3 places beyond it in the normal alphabet

Plain: **ABCDEFGHIJKLMNOPQRSTUVWXYZ**
Cipher: **DEFGHIJKLMNOPQRSTUVWXYZABC**

Generalization of Caesar Cipher

- 1) Replace each letter by the number to which it corresponds (its position in the alphabet)
- 2) **PERFORM SOME ARITHMETIC ON THE NUMBER, REDUCING MODULO THE NUMBER OF CHARACTERS IN THE ALPHABET**
- 3) Replace resulting number by its letter equivalent

Step 2:

Caesar: Add 3

Other Possibilities?

Step 2:
Caesar: Add 3
Other Possibilities?

Add k for some other integer k

How many choices are there for k that produce different cipher texts?

$k = 1, 2, 3, \dots, n - 1$ where n is the number of letters in the alphabet.

Step 2:
Caesar: Add 3
Other Possibilities?

Add k for some other integer k

How many choices are there for k that produce different cipher texts?

$k = 1, 2, 3, \dots, n - 1$ where n is the number of letters in the alphabet.

Caesar Cipher with shift k .

Suppose you know that the general method was such a shift but you do not know k .

Generalization of Caesar Cipher

- 1) Replace each letter by the number to which it corresponds (its position in the alphabet)
- 2) **PERFORM SOME ARITHMETIC ON THE NUMBER, REDUCING MODULO THE NUMBER OF CHARACTERS IN THE ALPHABET**
- 3) Replace resulting number by its letter equivalent

Generalization of Caesar Cipher

- 1) Replace each letter by the number to which it corresponds (its position in the alphabet)
- 2) **PERFORM SOME ARITHMETIC ON THE NUMBER, REDUCING MODULO THE NUMBER OF CHARACTERS IN THE ALPHABET**
- 3) Replace resulting number by its letter equivalent

Step 2:

Caesar: Shift Add k

Other Possibilities?

Multiply?

A	1	3	C	N	14	42	16	P
B	2	6	F	O	15	45	19	S
C	3	9	I	P	16	48	22	V
D	4	12	L	Q	17	51	25	Y
E	5	15	O	R	18	54	2	B
F	6	18	R	S	19	57	5	E
G	7	21	U	T	20	60	8	H
H	8	24	X	U	21	63	11	K
I	9	27	1	A	22	66	14	N
J	10	30	4	D	23	69	17	Q
K	11	33	7	G	24	72	20	T
L	12	36	10	J	25	75	23	W
M	13	39	13	M	26	78	26	Z

ABCDEFGHIJKLMNOPQRSTUVWXYZ

CFILORUXADGJMP SVYBEHKNQ TWZ

Multiply by 2?

A	1	2	B	N	14	28	2	B
B	2	4	D	O	15	30	4	D
C	3	6	F	P	16	32	6	F
D	4	8	H	Q	17	34	8	H
E	5	10	J	R	18	36	10	J
F	6	12	L	S	19	38	12	L
G	7	14	N	T	20	40	14	N
H	8	16	P	U	21	42	16	P
I	9	18	R	V	22	44	18	R
J	10	20	T	W	23	46	20	T
K	11	22	V	X	24	48	22	V
L	12	24	X	Y	25	50	24	X
M	13	26	Z	Z	26	52	26	Z

ABCDEFGHIJKLMNOPQRSTUVWXYZ

BDFHJLNPRTVXZBDFHJLNPRTVXZ

MULTIPLICATION BY 2

A, N $\rightarrow$ B B, O $\rightarrow$ D C, P $\rightarrow$ F

ABC $\rightarrow$ BDF

ABP $\rightarrow$ BDF

AOC $\rightarrow$ BDF

AOP $\rightarrow$ BDF

NBC $\rightarrow$ BDF

NPB $\rightarrow$ BDF

NOC $\rightarrow$ BDF

NOP $\rightarrow$ BDF

Problem:

MULTIPLICATION BY 2

A, N → B B, O → D C, P → F

ABC → BDF

ABP → BDF

AOC → BDF

AOP → BDF

NBC → BDF

NPB → BDF

NOC → BDF

NOP → BDF

Problem: HOW DO WE GO
FROM ENCIPHERED
MESSAGE BACK TO THE
PLAINTEXT MESSAGE?

A MORE EXTREME CASE

MULTIPLY BY 13

A C E G I K M O Q S U W Y → M

B D F H J L N P R T V X Z → Z

MZMZMMZMMM

CAN BE DECIPHERED AS

EVIL MEN SAY OR

STATISTICS

$$13^{10} = 13,858,491,849$$

What about Multiplication?

$$f(x) = a \cdot x \bmod N$$

a multiplier

N size of alphabet

$$S : \{1, 2, \dots, N\}$$

1) Does $f : S \rightarrow S$?

2) When is f one-to-one?

$$x \neq y \Rightarrow f(x) \neq f(y)$$

Suppose $f(x) = f(y)$

$$ax \bmod N = ay \bmod N$$

$$ax \equiv ay \bmod N$$

$$a(x - y) \equiv 0 \bmod N$$

This implies $x \equiv y$ exactly when a is relatively prime to N .

Our Arithmetic Function Must Be Reversible
One- To - One
Have an Inverse

$$S : \{1, 2, \dots, 26\}$$

Caesar: $f(x) = x + 3(\text{mod}26)$

What is Inverse?

General shift: $f(x) = x + s(\text{mod}26)$

There are 26 possible shifts.

There are $26! = 4.03 \cdot 10^{26}$ different monoalphabetic substitution schemes

Number of Rearrangements of the English Alphabet

Choices for A: 26

Choices for B: 25

Choices for A and B: $26 \cdot 25 = 650$

Choices for C: 24

Choices for A, B, C: $26 \cdot 25 \cdot 24$

Choices for A, B, C, ..., Z:
 $26 \cdot 25 \cdot 24 \cdot 23 \cdot \dots \cdot 3 \cdot 2 \cdot 1 = 26!$

How Big is 26! ?

403291461126605635584000000

Brute Force Method

Check 1 million per second:

$$\frac{4.03 \cdot 10^{26}}{10^6} = 4.02 \cdot 10^{20} \text{ seconds}$$

How Big is 26! ?

403291461126605635584000000

Brute Force Method

Check 1 million per second:

$$\frac{4.03 \cdot 10^{26}}{10^6} = 4.02 \cdot 10^{20} \text{ seconds}$$

$$1.2 \cdot 10^{13} \text{ years}$$

Age of Universe: 10^9 years