Caesar Cipher

Martzel Baste

Definition

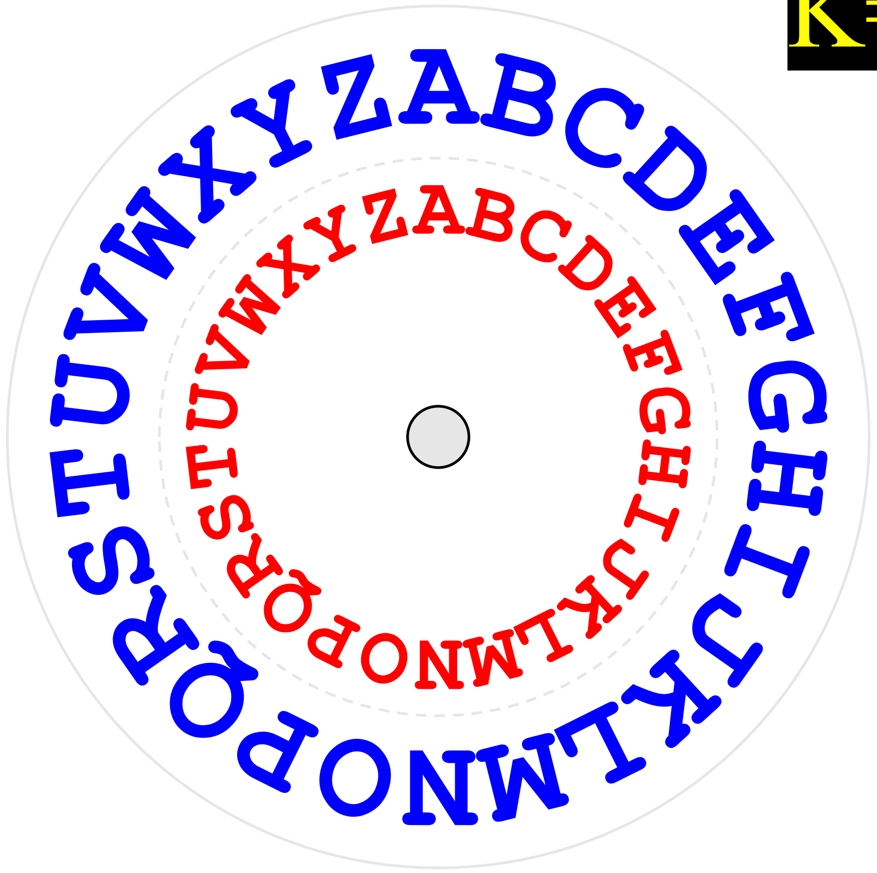
is a substitution cipher, named after **Julius Caesar**.

Operation principle: each letter is translated into the letter *a fixed number of positions* after it in the alphabet table.

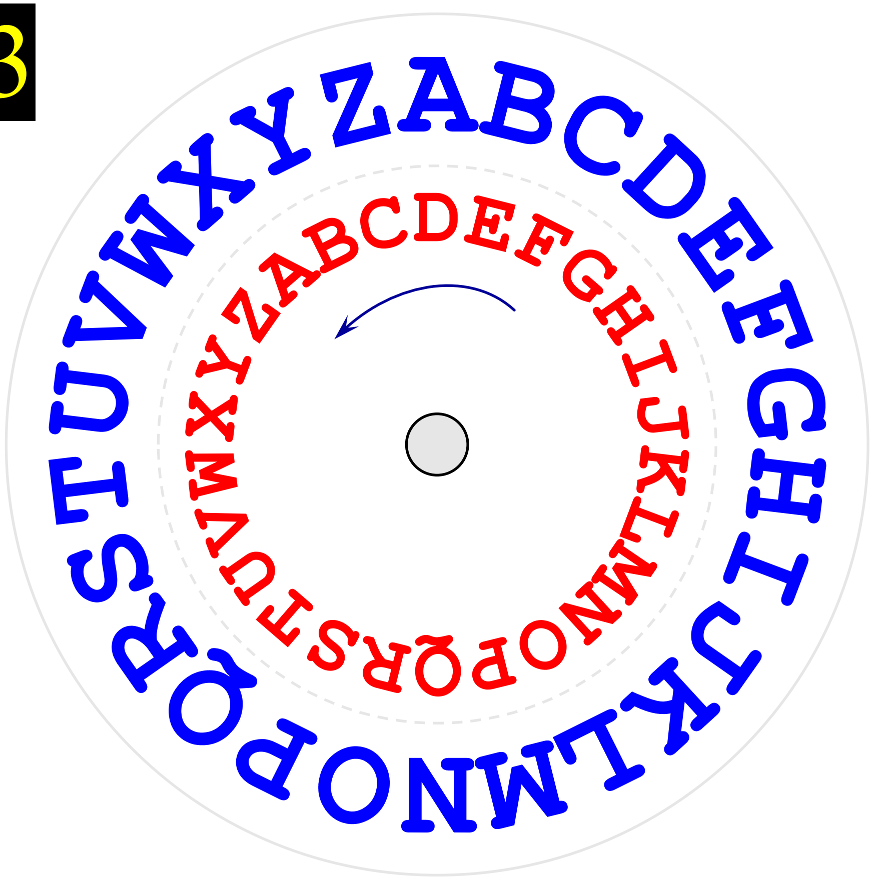
the fixed number of positions is a **key** both for encryption and decryption.

Operation principle

- Outer: plaintext
- Inner: ciphertext



K=3



Usage

The Caesar cipher is still useful to prevent people from unintentionally reading something.

- ROT-13
- By decrypting, the user agrees that they want to view the content.

Fundamental problem: key length is shorter than the message.

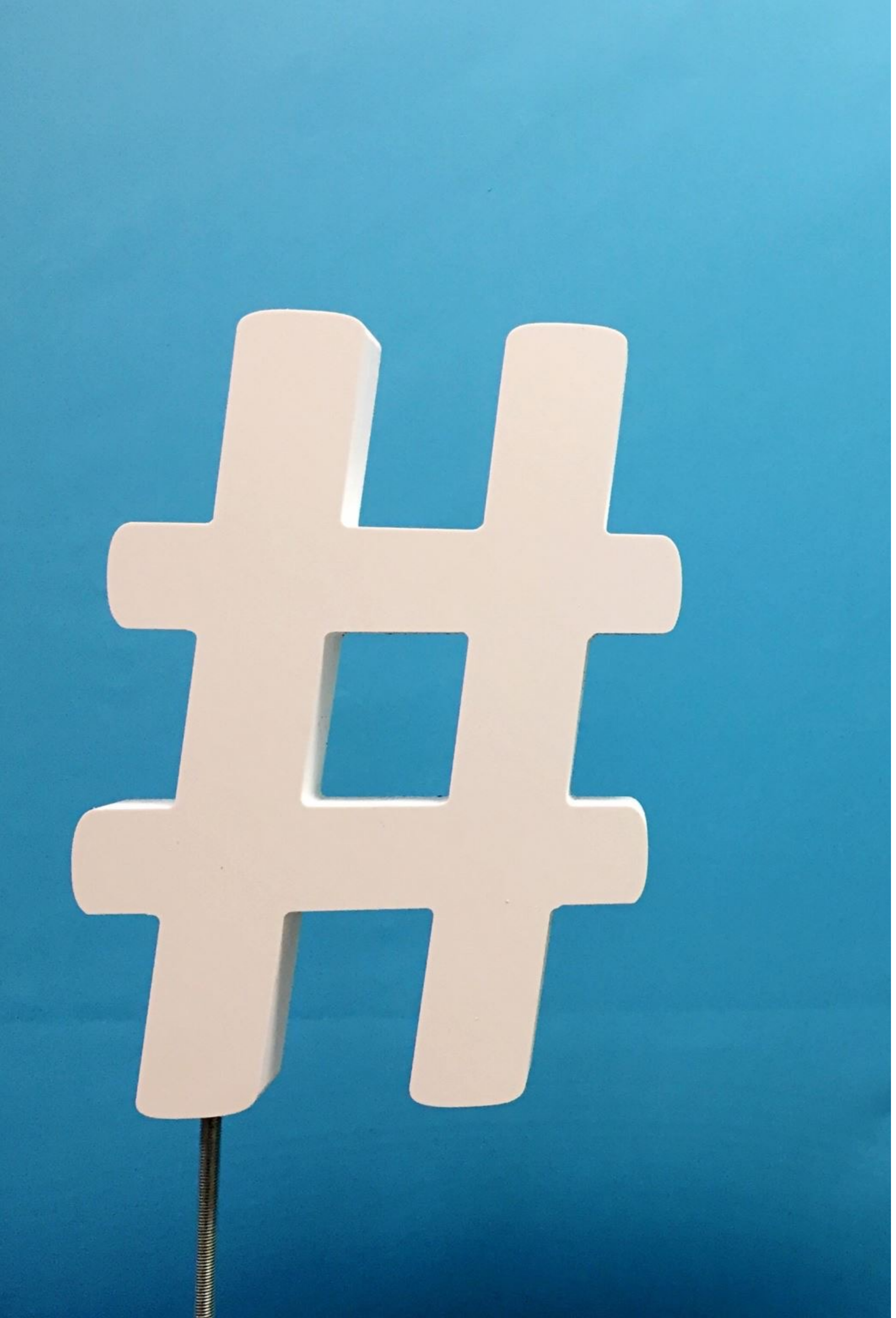
Let $\mathcal{P} = \mathcal{C} = \mathcal{K} = \mathbf{Z}_{26}$

$\forall x \in \mathcal{P}, \forall y \in \mathcal{C}, \forall K \in \mathcal{K}$, define

$y = e_K(x) = x + K$ (mod 26)

and

$X = d_K(y) = y - K$ (mod 26)



Example

K=4

```
Plaintext letter  : ABCDEF...UVWXYZ
Ciphertext letter : EFGHIJ...YZABCD
```

Hence

```
        MARTZEL BASTE
```

is translated into

```
        QEVXDIP FEWXI
```

Breaking the Caesar cipher

by trial-and error

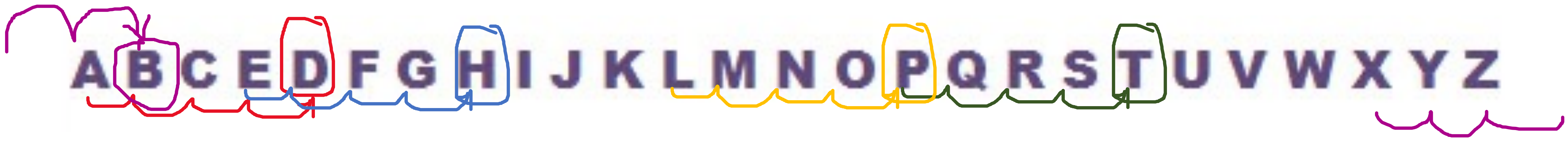
by using statistics on letters

- frequency distributions of letters

letter	percent
A	7.49%
B	1.29%
C	3.54%
D	3.62%
E	14.00%

…………………………………

Encryption And Decryption (Simple Shift)



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

APPLEX K→4

DTTPHB

Encryption And Decryption (Mathematical)

A	B	C	E	D	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	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

M every letter in the message.

X number order of each letter in the alphabet from 0 to 25.

K the key-value

Y the number result upon adding X and K

Convert the letter **M** into the number **X** that matches its order in the alphabet starting from 0 to 25.

Convert the number **Y** into a letter **M** that matches its order in the alphabet starting from 0 to 25.

Calculate: $Y = (X + K) \bmod 26$

Encryption And Decryption (Mathematical)

A	B	C	E	D	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	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

1. Convert the letter M into the number X that matches its order in the alphabet starting from **0 to 25**.
2. Calculate: ***Y* = *(X + K) mod 26***
3. Convert the number **Y into a letter M** that matches its order in the alphabet starting from 0 to 25.

$$\begin{array}{rcccccc}
 & A & P & P & L & E & X \qquad K \to 4 \\
 & 0 & 15 & 15 & 11 & 3 & 23 \\
+ & 4 & 4 & 4 & 4 & 4 & 4 \\
\hline
 & (4 & 19 & 19 & 5 & 7) & \text{mod } 26 \\
\hline
 & 4 & 19 & 19 & 15 & 7 & \underline{1} \\
 & D & T & T & P & H & B
\end{array}$$

$$\left.\begin{array}{c} 23 \\ 4 \end{array}\right\} 27$$

Decryption (Modular Math)

A	B	C	E	D	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	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

1. Let **C** every letter in the ciphertext. Convert the letter **C** into the number **X** that matches its order in the alphabet starting from **0 to 25**.
2. Calculate: ***Y* = *(X - K) mod 26***
3. Convert the number **Y into a letter C** that matches its order in the alphabet starting from 0 to 25.

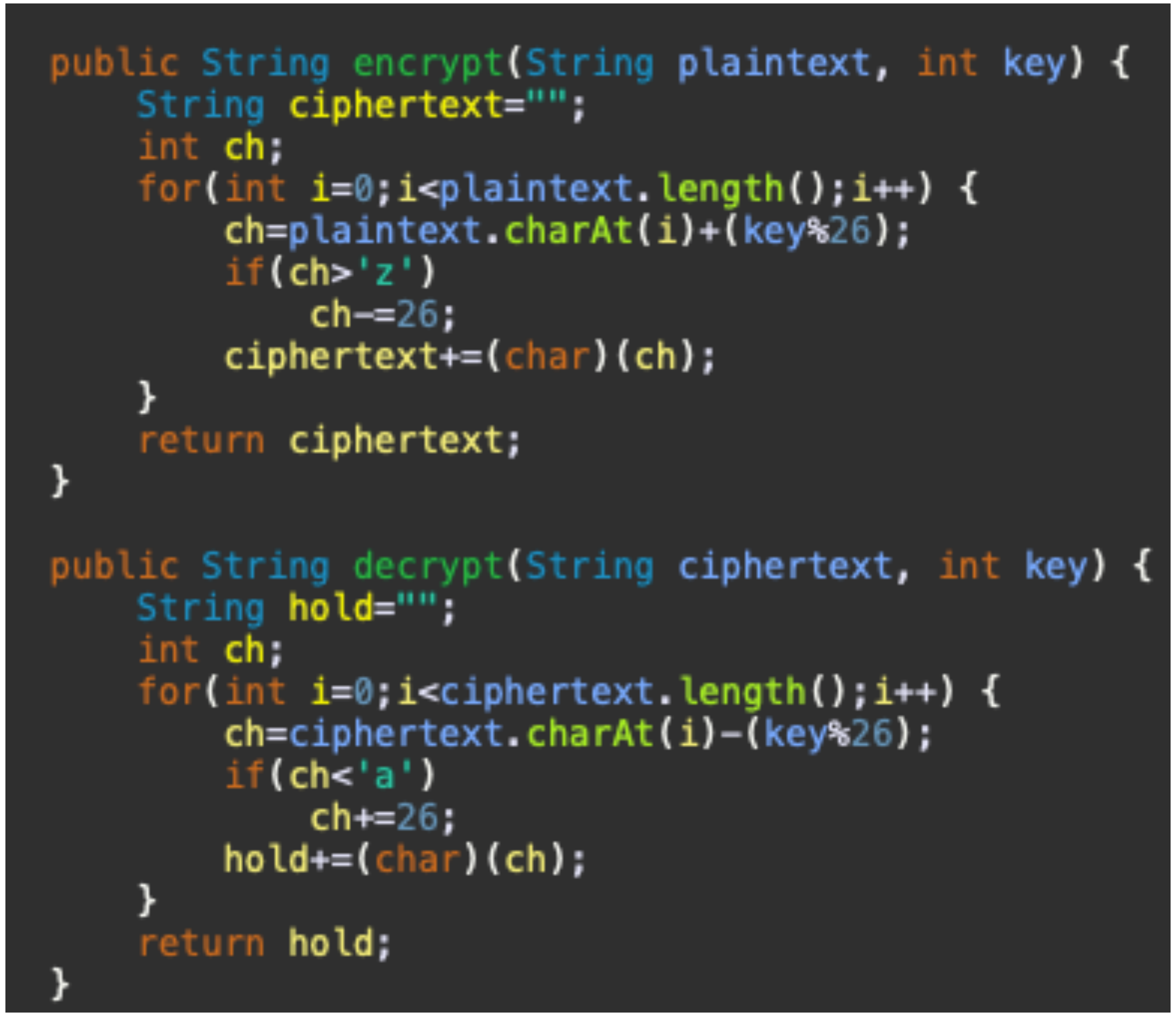
D T T P H B

$K \rightarrow 4$

$$\begin{array}{rrrrrrr}
 & 4 & 19 & 19 & 15 & 7 & 1 \\
- & 4 & 4 & 4 & 4 & 4 & 4 \\
\hline
 & (0 & 15 & 15 & 11 & 3 & -3) \bmod 26 \\
\hline
 & 0 & 15 & 15 & 11 & 3 & 23
\end{array}$$

A P P L E X

Sample Program



```java
public String encrypt(String plaintext, int key) {
    String ciphertext="";
    int ch;
    for(int i=0;i<plaintext.length();i++) {
        ch=plaintext.charAt(i)+(key%26);
        if(ch>'z')
            ch-=26;
        ciphertext+=(char)(ch);
    }
    return ciphertext;
}

public String decrypt(String ciphertext, int key) {
    String hold="";
    int ch;
    for(int i=0;i<ciphertext.length();i++) {
        ch=ciphertext.charAt(i)-(key%26);
        if(ch<'a')
            ch+=26;
        hold+=(char)(ch);
    }
    return hold;
}
```