Vigenere Cipher

Tam

Basic knowledge

Simple substitution cipher

The most famous example: the Caesar cipher.

Example: Shift one character.

```
H A L
↓ ↓ ↓
I B M
```

Simple substitution cipher is

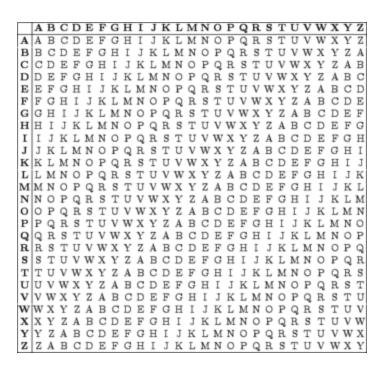
each 'H' of plain text become the same charactor.

Vigenere Cipher

Vigenere Cipher

plain text: 'CODE'

key: 'ARM'



cipher text: 'CFPE'

Using Computer

We assume the below:

P_i \$\$: The i-rd charactor of plain text

\$\$ K_i \$\$: The i-rd charactor of key

\$\$ C_i \$\$: The i-rd character of ciphered text

$$SC_i = (P_i + K_i) \mod 26$$

$$P_i = (C_i - K_i) mod 26$$

Kasisky Test

Babbage found the below:

- 1. Search for strings of the same characters.
- 2. Count the intervals between the strings.
- 3. Calculate the common factors of these numbers.
 - For example: we found the intervals number are 9, 63, 180, we can calculate the common factors of these numbers are 3 or 9.
- 4. We can guess the length of the key is 3 or 9.
- 5. We run it through frequency analysis.

Finally, this is the same as the Caesar cipher with intervals of 3 or 9.

Charles Babbage

- The father of computer.
- discover the steam calculator "Babbage machine".



autokey cipher

Basic Idea

Plaintext: attackatdawn

OrigKey: QUEENLY

Key: QUEENLYATTACKATDAWN

Ciphertext: QNXEPVYTWTWP

Ciphertext: QNXEPVYTWTWP

OrigKey: QUEENLY

Plaintext: a

Key: QUEENLYA

Vigenere Cipher