# **Vigenere Cipher**

Vigenere Cipher

## **Basic knowledge**

#### Simple substitution cipher

The most famous example: the Caesar cipher.

Example: Shift one character.

HAL

 $\downarrow$   $\downarrow$   $\downarrow$ 

IBM

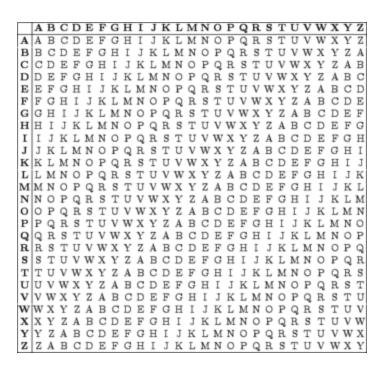
Simple substitution cipher is each 'd' of plain text become the same charactor.

2

## **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

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

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

## **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 is 3 or 9.
- 4. We can find 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.