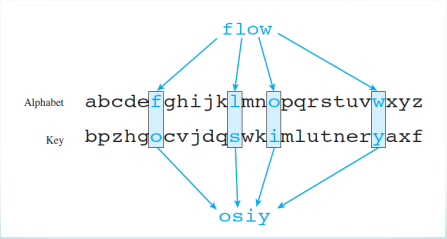
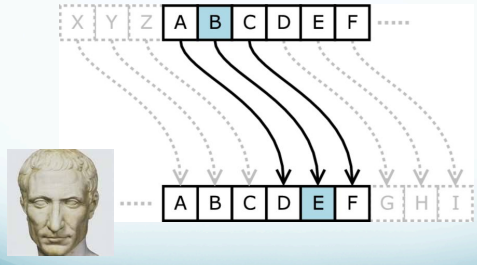
# Substitution Ciphers

CMPUT 396

## Substitution cipher




## Caesar cipher






Julius Caesar

## Caesar's memoirs

- Cicero receives Caesar's message (*De Bello Gallico* V:XLVIII:IX i.e. *The Gallic Wars* 5.48.9)
- Original Latin*: Ille perlectam in conventu militum recitat maximaque omnes laetitia adficit.*
- Google Translate: *He read it in the assembly of the greatest joy.*
- Human translation: *He, after perusing it, reads it out in an assembly of the soldiers, and fills all with the greatest joy.*

## Caesar's cipher wheel

Each ciphertext letter is "the sum" of the plaintext letter and the shift value:

$C_i = M_i + K \bmod 26$

| A | B | C | D | E | 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 |

| I | W | T | | C | T | L | | E | P | H | H | L | D | G | S | | X | H | | H | L | D | G | S | U | X | H | W |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| ↓ | ↓ | ↓ | ↓ | ↓ | ↓ | ↓ | ↓ | ↓ | ↓ | ↓ | ↓ | ↓ | ↓ | ↓ | ↓ | ↓ | ↓ | ↓ | ↓ | ↓ | ↓ | ↓ | ↓ | ↓ | ↓ | ↓ | ↓ |
| T | H | E | | N | E | W | | P | A | S | S | W | O | R | D | | I | S | | S | W | O | R | D | F | I | S | H |

## The Vigenere square