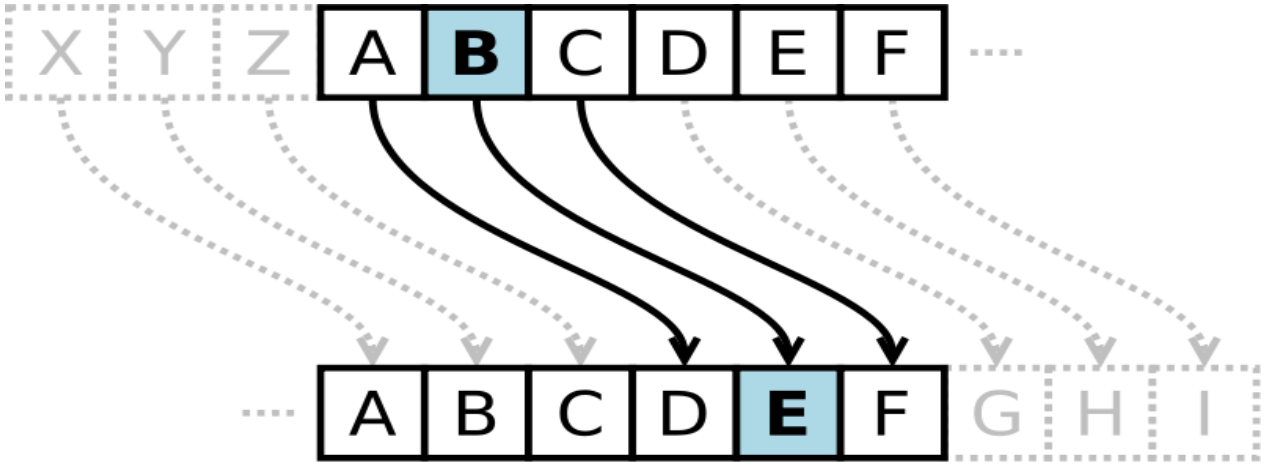
Caesar Cipher

- In cryptography, a **Caesar cipher**, also known as a **Caesar's cipher**, the **shift cipher**, **Caesar's code** or **Caesar shift**, is one of the simplest and most widely known encryption techniques.
- It is a type of substitution cipher in which each letter in the plaintext is replaced by a letter some fixed number of positions down the alphabet.
- For example, with a shift of 3, A would be replaced by D, B would become E, and so on.



Caesar Cipher (Conti…)

- The encryption can also be represented using modular arithmetic by first transforming the letters into numbers, according to the scheme, A = 0, B = 1,..., Z = 25.
- Encryption of a letter by a shift *n* can be described mathematically as

$$E_n(x) = (x + n) \mod 26.$$

- Decryption is performed similarly,

$$D_n(x) = (x - n) \mod 26.$$