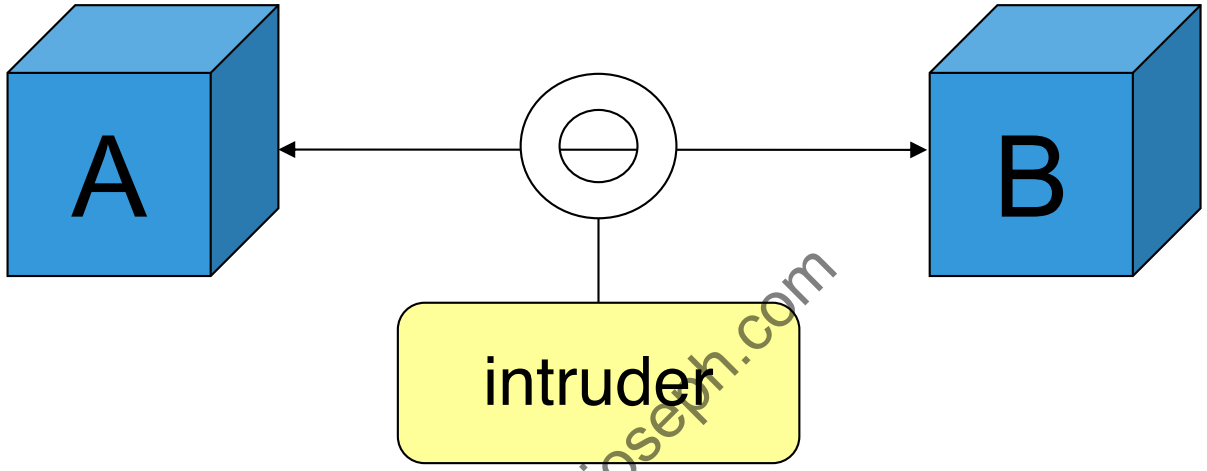
Cryptography

- *Cryptography is the study of mathematical techniques related to aspects of information security, such as confidentiality, data integrity, entity authentication, and data origin authentication*

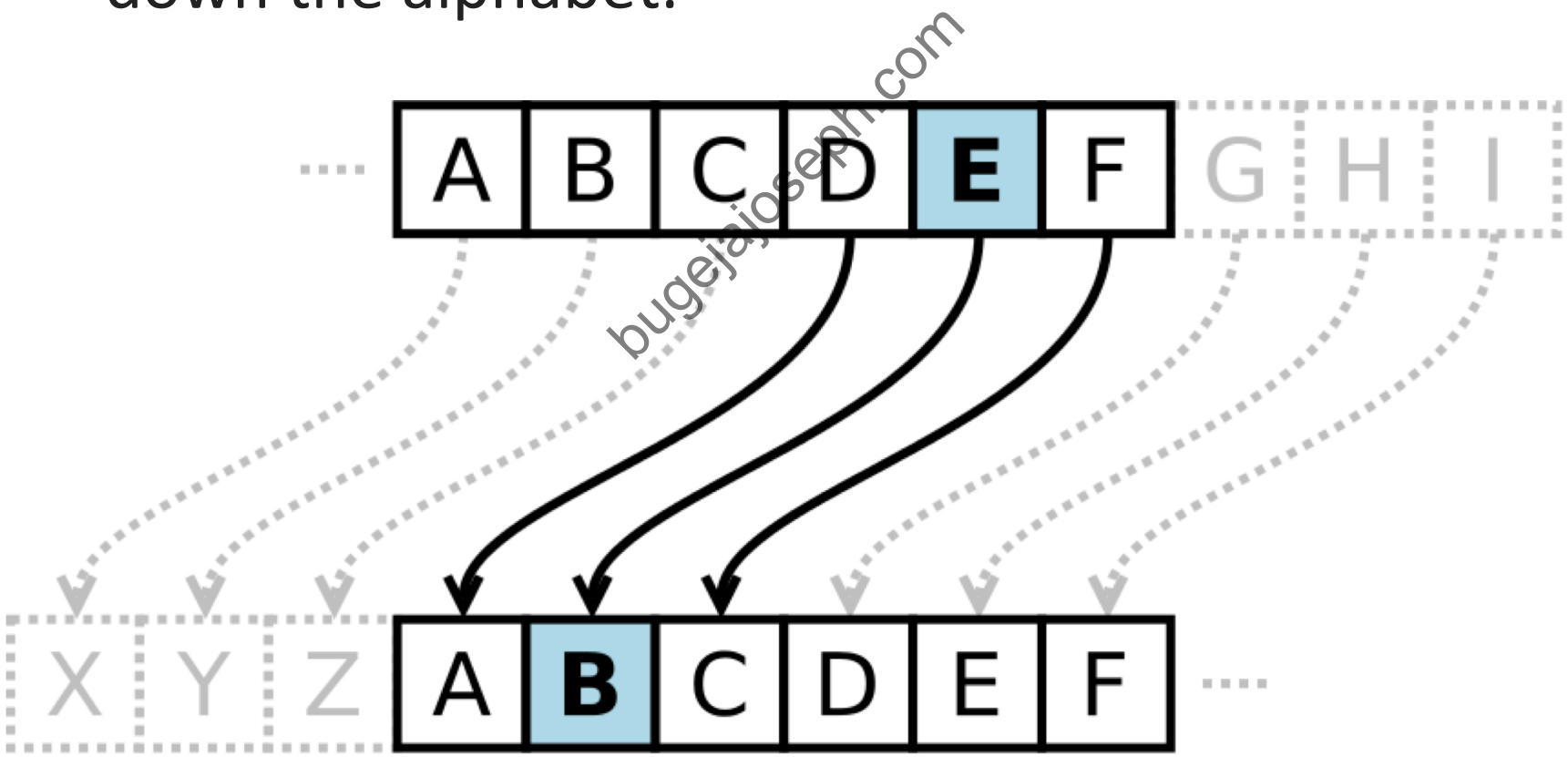
Old Paradigm



- *A* and *B* trust each other
- *A* and *B* communicate over an insecure channel
- Intruder can read, delete, and insert messages
- With cryptography, *A* and *B* construct a secure logical channel over an insecure network

Caesar Cipher

- Replace each plaintext letter with a different one a fixed number of places (e.g. left shift of three) down the alphabet.



Caesar Cipher

- 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.

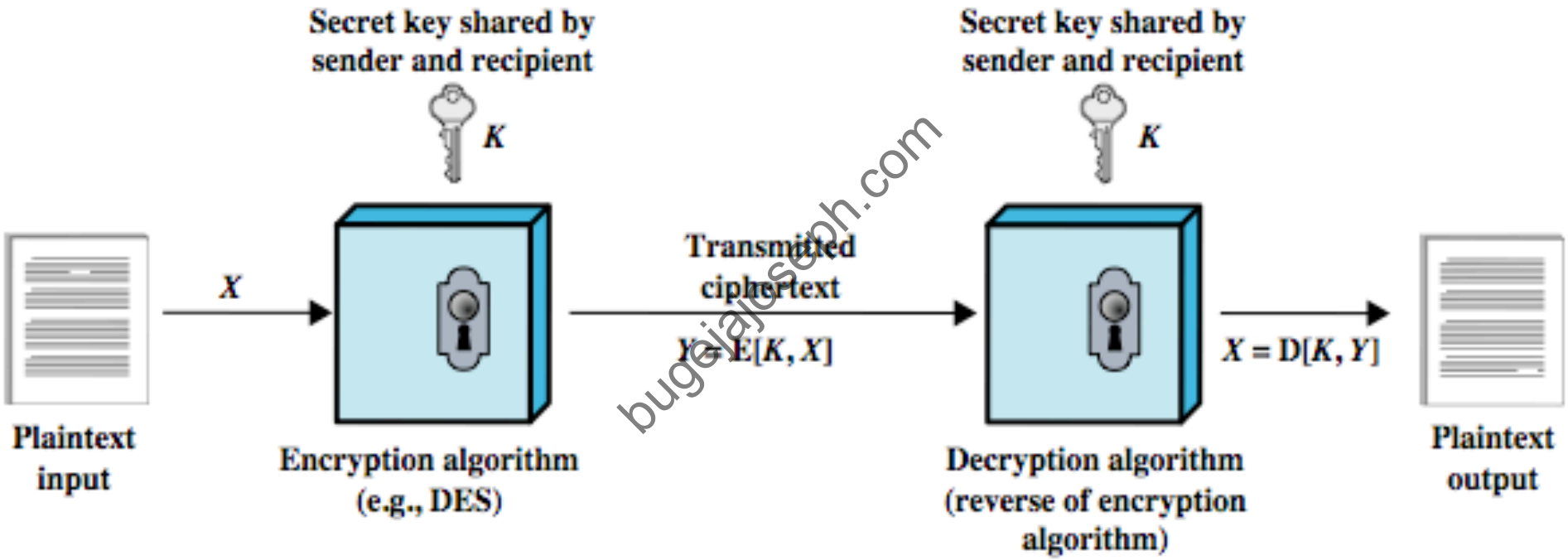
- Encryption of a letter *x* by a shift *n* can be described mathematically as:

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

- Decryption is performed similarly:

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

Symmetric Encryption



Public-Key Encryption