INTRODUCTION TO ENCRYPTION

AIF 183134-02 PRIVASI DATA
UNIVERSITAS KATOLIK PARAHYANGAN

Mariskha Adithia, SSi, MSc, PDEng

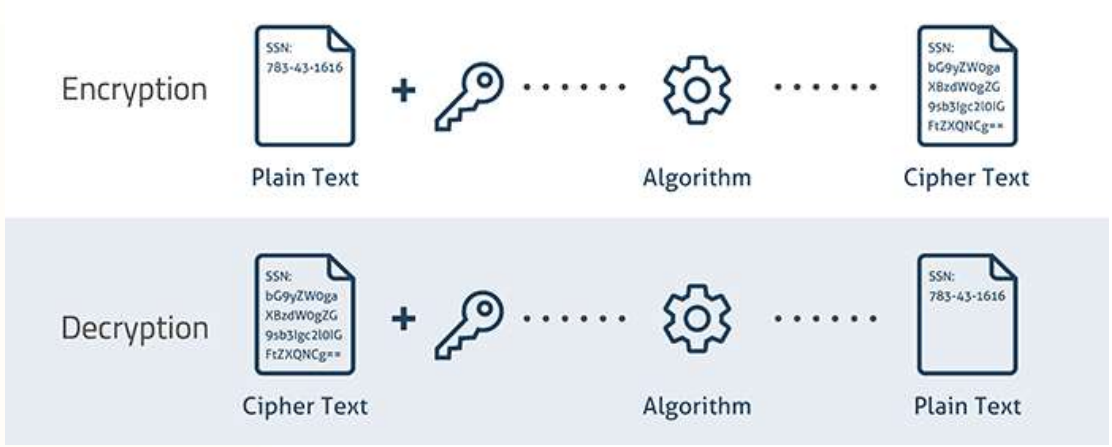
INFORMATIKA UNPAR

ENCRYPTION X PRIVACY

Encryption

INFORMATIKA
UNPAR

KRIPTOGRAFI – KERAHASIAAN



TERMINOLOGIES
PLAINTEXT AND CIPHERTEXT

- **Plaintext** is data or information which can be read and understood
- **Ciphertext or cryptogram** is data or information that has been coded

Example:

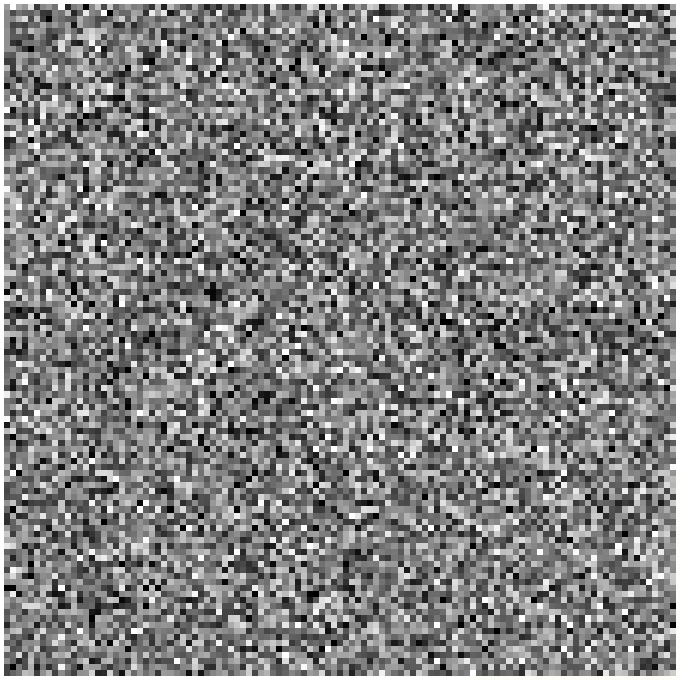
Plaintext ⟶ SEKOLAH

Ciphertext ⟶ UGMQNCJ

INFORMATIKA UNPAR

TERMINOLOGIES

PLAINTEXT AND CIPHERTEXT (2)



INFORMATIKA UNPAR

TERMINOLOGIES

ENCRYPTION AND DECRYPTION

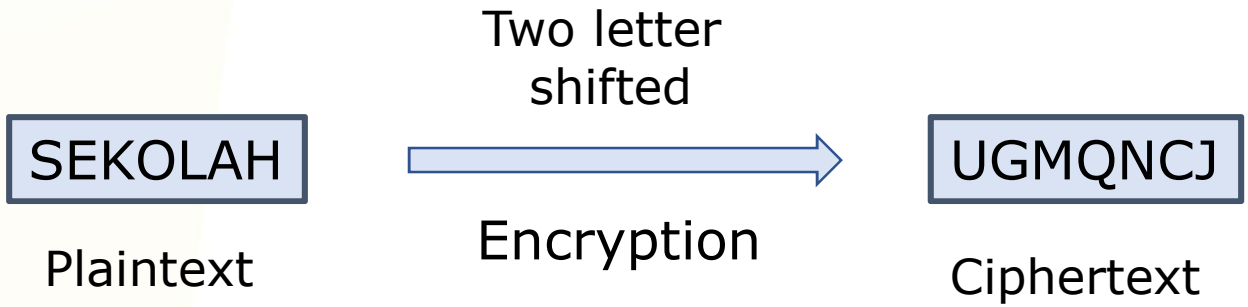
- **Encryption or enciphering** is a process to transform plaintext to ciphertext
- **Decryption or deciphering** is a process to transform ciphertext back to plaintext

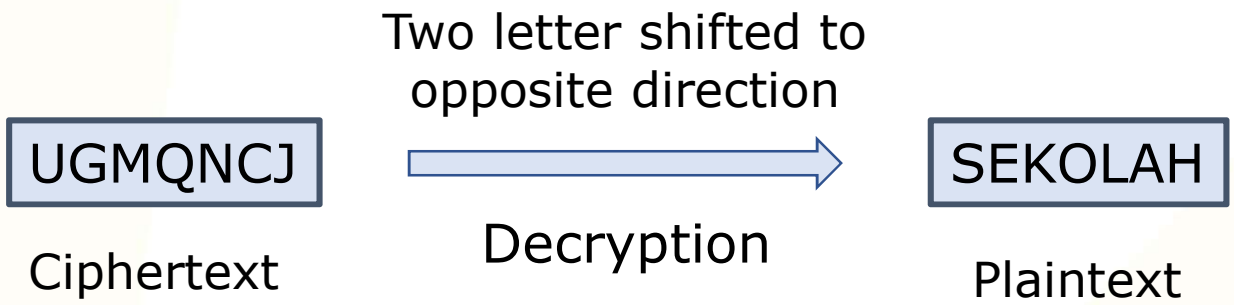
INFORMATIKA UNPAR

TERMINOLOGIES

ENCRYPTION AND DECRYPTION

Example:





INFORMATIKA UNPAR

TERMINOLOGIES
ALGORITHM AND KEY

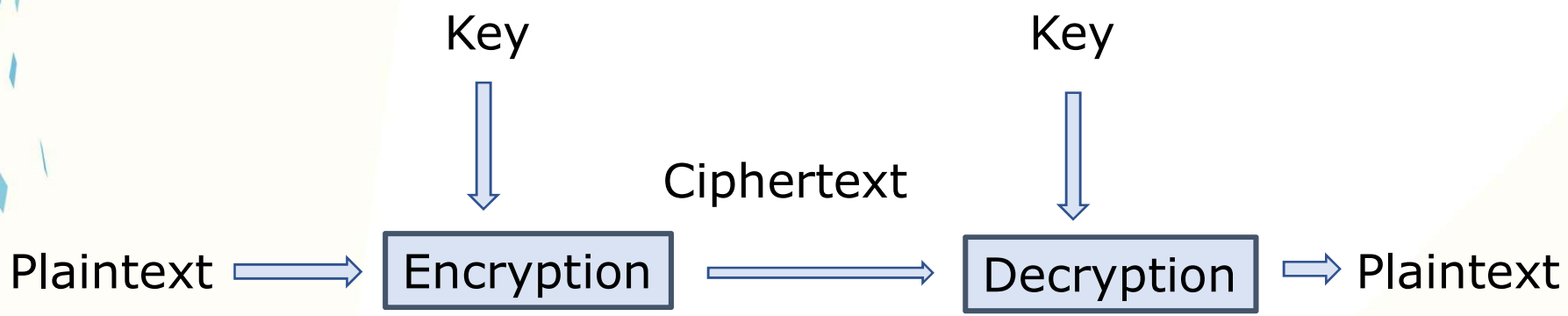
- **Cryptographic algorithm** is a set of mathematical function used for encryption and decryption
- **Key** is a parameter used for encryption and decryption

INFORMATIKA UNPAR

TERMINOLOGIES

ALGORITHM AND KEY (2)

Encryption and decryption scheme:



INFORMATIKA UNPAR

TERMINOLOGIES

ALGORITHM AND KEY (3)

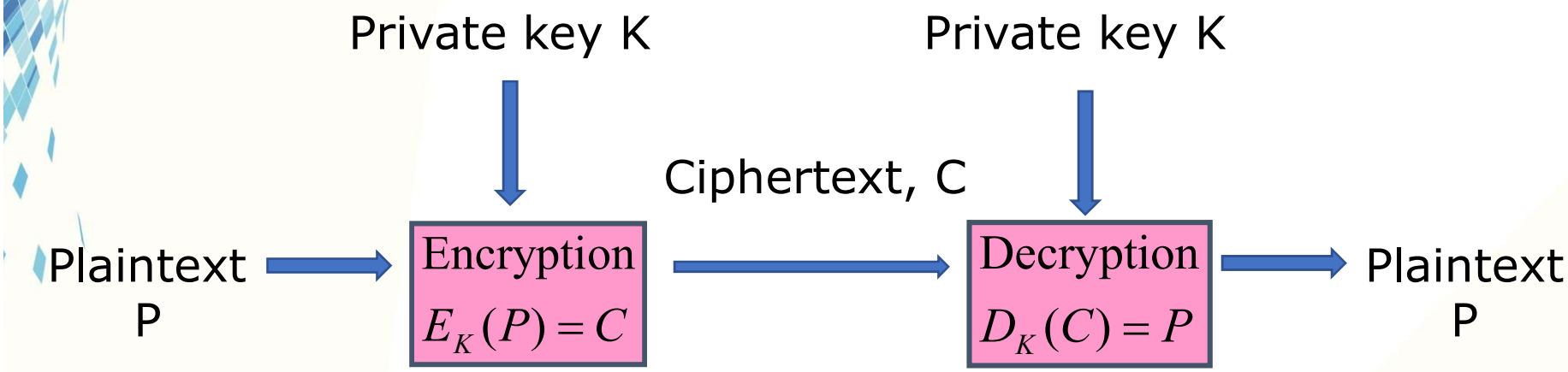
Example:

INFORMATIKA UNPAR

SYMMETRIC KEY CRYPTOGRAPHY

- Encryption and decryption key is the same
- DES, AES,Twofish, Blowfish, etc
- Weakneses:
  - Sender and receiver should have the same key. So?

SYMMETRIC KEY CRYPTOGRAPHY (2)



INFORMATIKA UNPAR

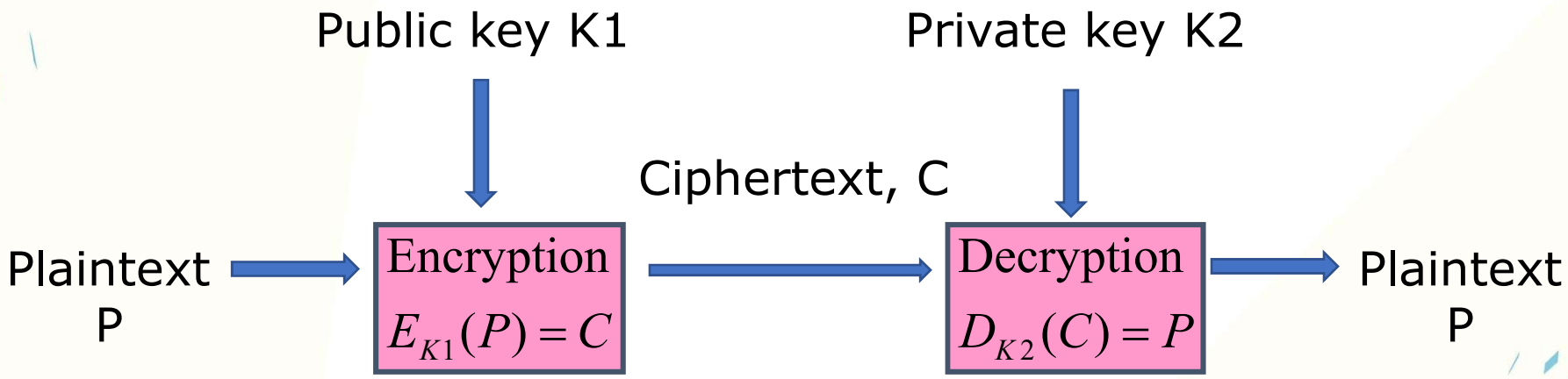
ASYMMETRIC KEY CRYPTOGRAPHY

- Public key cryptography
- Encryption: public key
- Decryption: private key
- Everybody has the public key, receiver has the private key
- RSA, ElGamal, DSA, etc

INFORMATIKA UNPAR

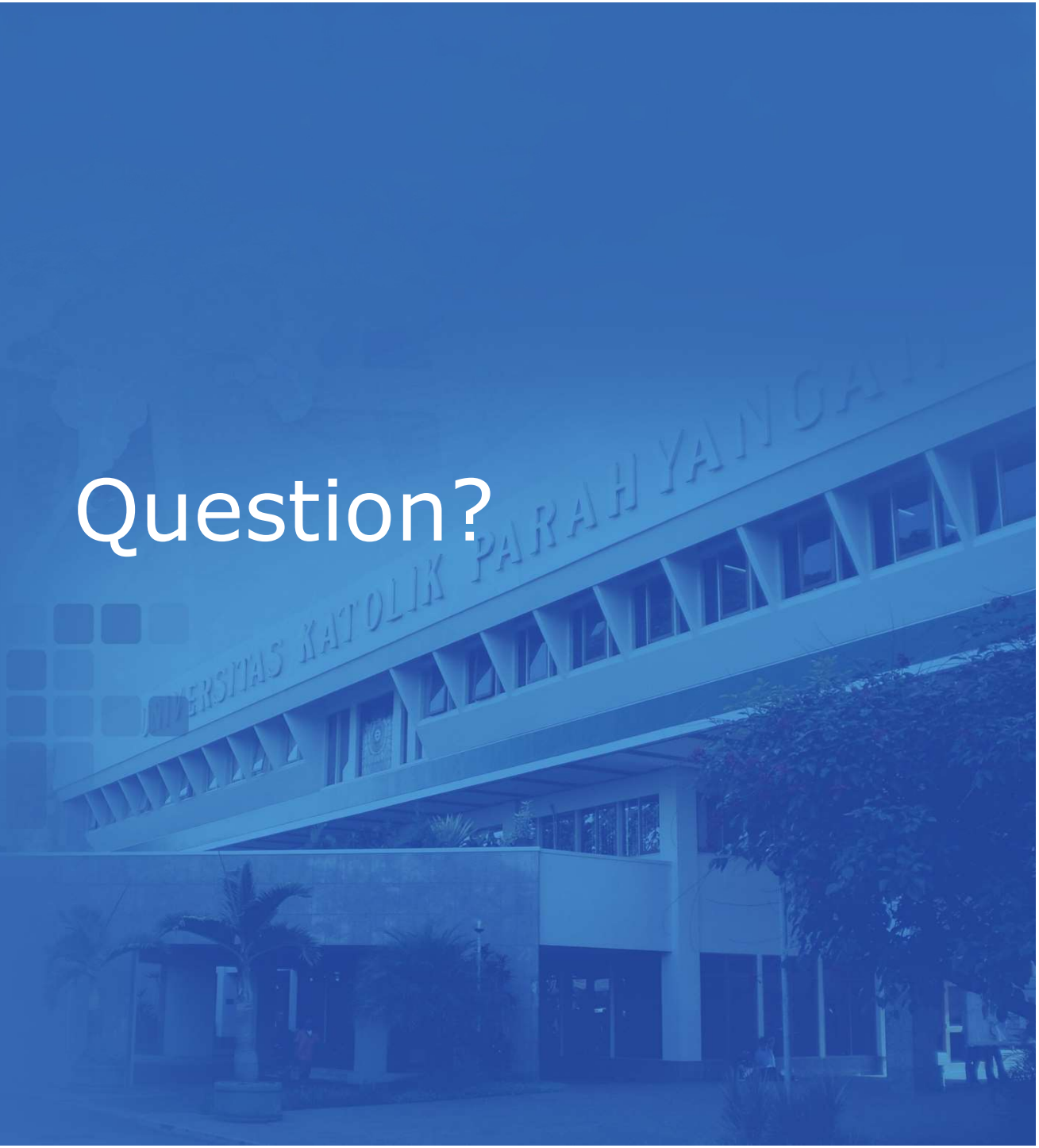
ASYMMETRIC KEY CRYPTOGRAPHY (2)

- Strength
  - Private key distribution is not needed
  - The number of key can be minimized



INFORMATIKA UNPAR

Question?



INFORMATIKA
UNPAR

informatika.unpar.ac.id
informatika@unpar.ac.id
facebook.com/if.unpar
@if_unpar