Cryptography

Martzel P. Baste

”kryptos" means "hidden” "graphy" stands for "writing."

Cryptography

- the science of using mathematics to encrypt and decrypt data.
- it enables you to store sensitive information or transmit it across unsecured networks (like the Internet) so that it cannot be read by anyone except the intended recipient.

Cryptography

THE ART OF SECRET WRITING

THE ART OF PROTECTION USING INFORMATION

THE SCIENCE OF ENCRYPTING OR HIDING *SECRETS*

NEEDED FOR CONFIDENTIALITY

Objectives

Confidentiality

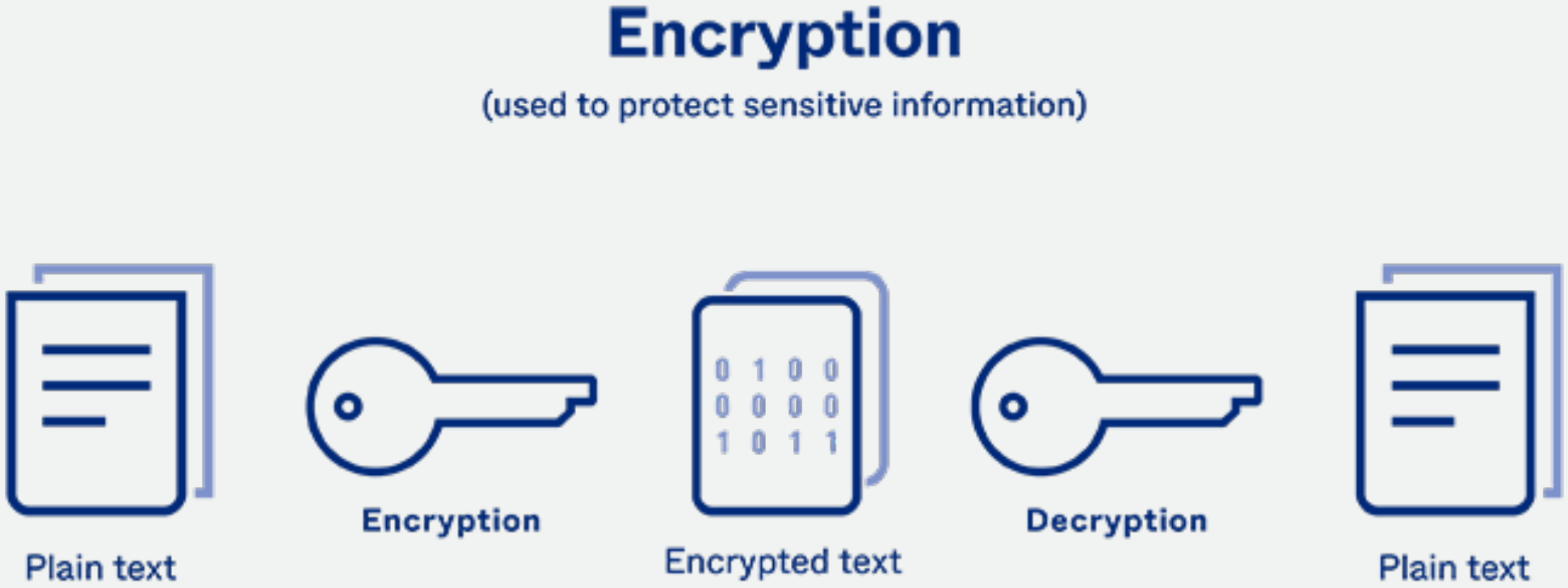
Integrity

Non-repudiation

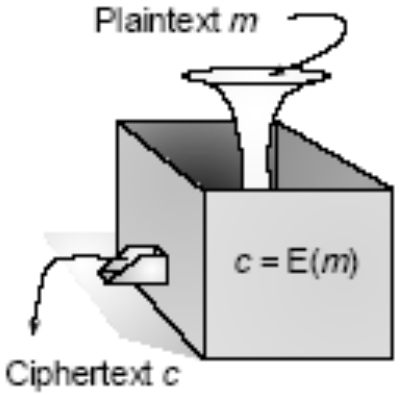
Authentication

plaintext	the original message
ciphertext	the coded message
cipher	algorithm for transforming plaintext to ciphertext
key	info used in cipher known only to sender/receiver
encipher (encrypt)	converting plaintext to ciphertext
decipher (decrypt)	recovering ciphertext from plaintext
cryptography	study of encryption principles/methods
cryptanalysis (codebreaking)	the study of principles/ methods of deciphering ciphertext *without* knowing key
cryptology	the field of both cryptography and cryptanalysis

Conventional Encryption

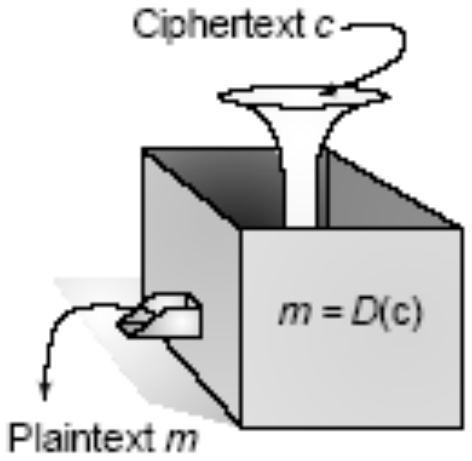


Encryption



The conversion of a original message, referred to as *plaintext* or *cleartext*, into a different message known as *ciphertext* (the word cipher comes from an old Arabic word meaning empty or zero), or *cryptogram*.

Decryption



The extraction process by which the intended receiver extracts the plaintext from the ciphertext

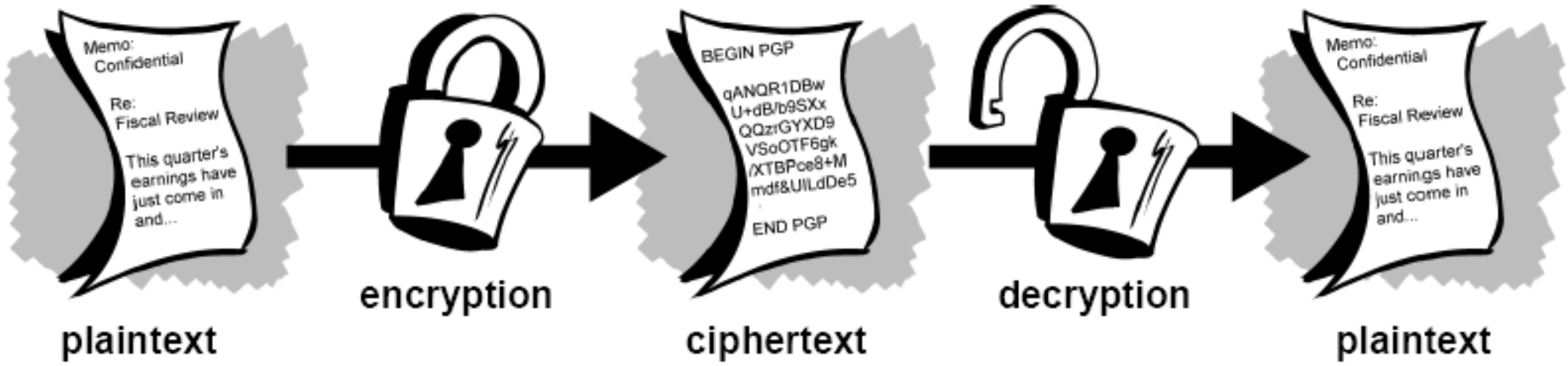
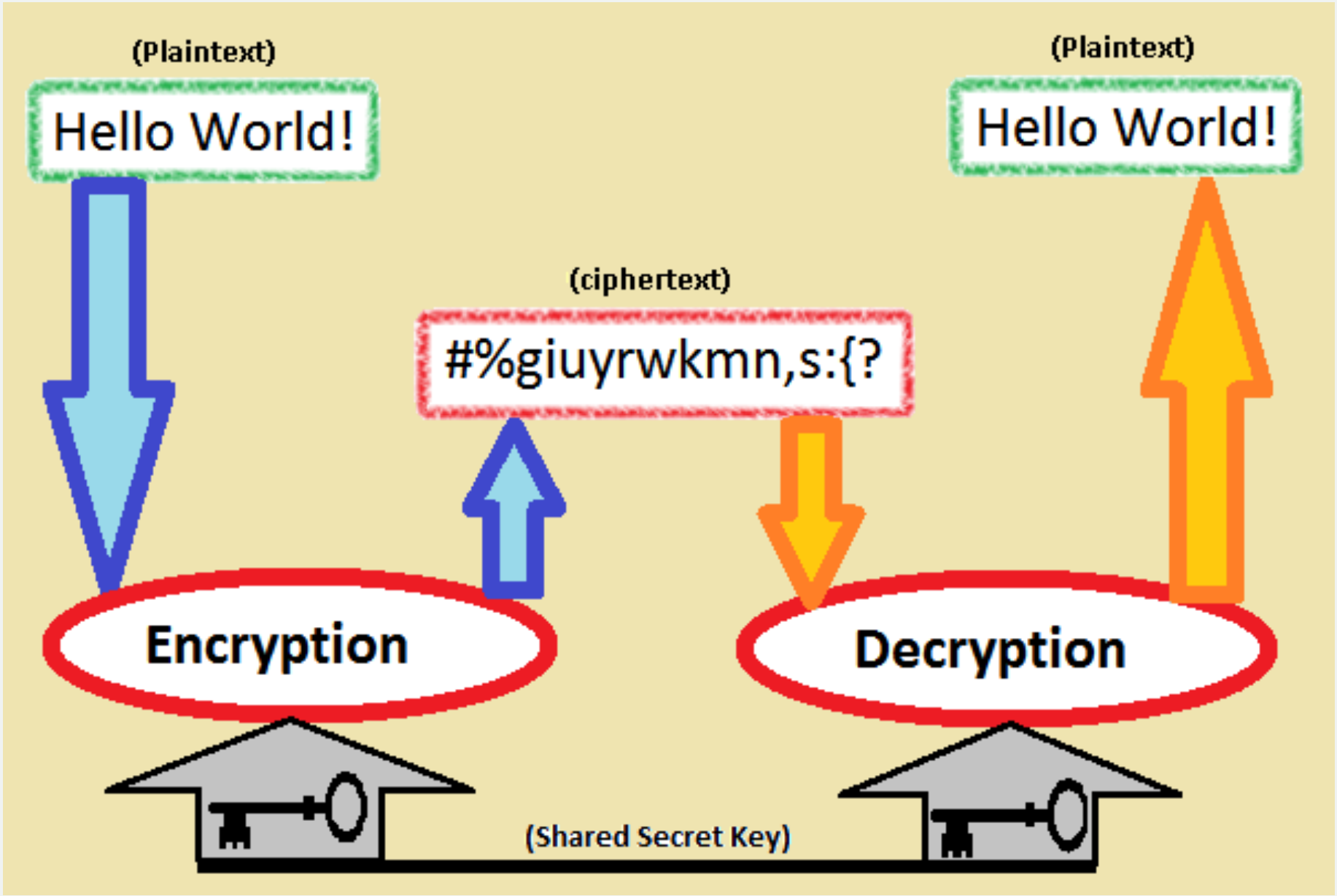
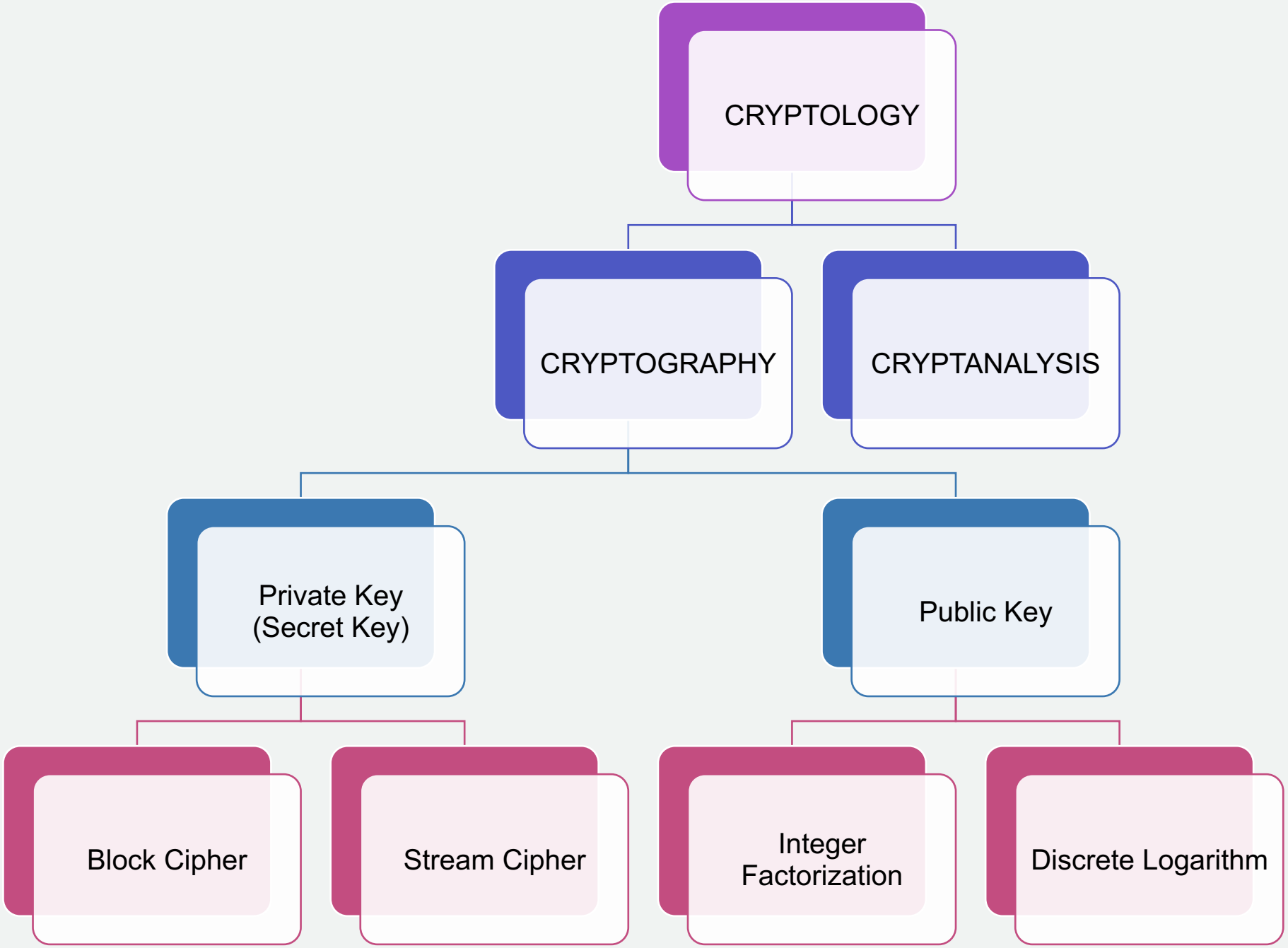
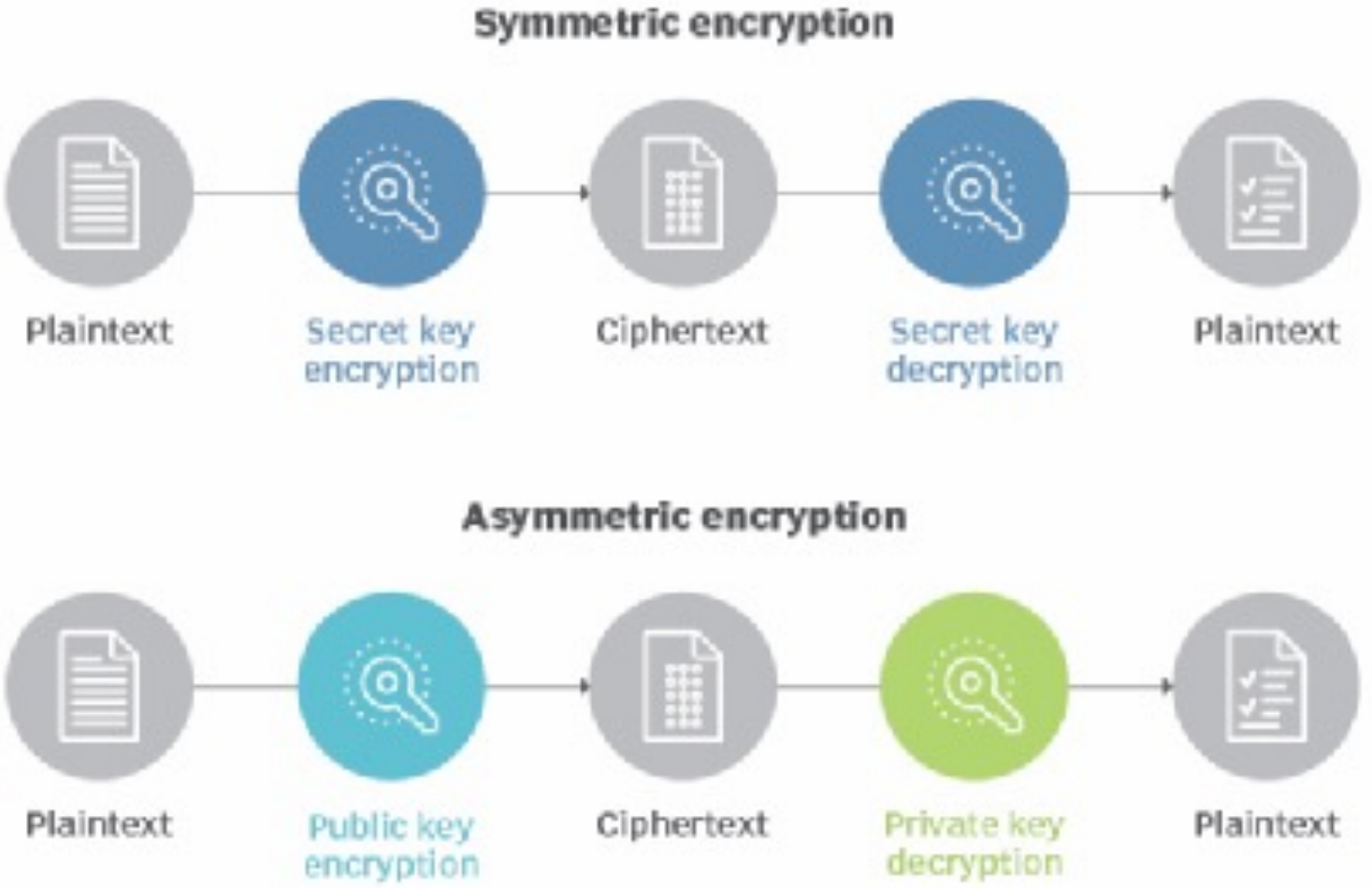


Figure 1-1. Encryption and decryption


(Plaintext)
Hello World!
(Plaintext)
Hello World!
(ciphertext)
#%giuyrwkmn,s:{?
Encryption
Decryption
(Shared Secret Key)


CRYPTOLOGY
CRYPTOGRAPHY
CRYPTANALYSIS
Private Key
(Secret Key)
Public Key
Block Cipher
Stream Cipher
Integer
Factorization
Discrete Logarithm

Symmetric vs. asymmetric encryption



Classical Cryptography

Monoalphabetic Ciphers

- Shift Cipher (Caesar Cipher)
- Substitution Cipher
- Affine Cipher

Polyalphabetic Ciphers

- Vigenère Cipher
- Hill Cipher
- Permutation Cipher

Benefits of Cryptography