



COMP2003J Introduction to Network Security

Soumyabrata DEV

School of Computer Science
University College Dublin

<https://soumyabrata.dev/>

Beijing-Dublin International College (BDIC)
29-April-2021

Course website is available here:

<https://soumyabrata.dev/bdic.html>



[Home](#)

COMP2003J Introduction to Network Security

Date: 29-April-2021

Time: 16:15 hours

Duration: 5 minutes (approximately)

Venue: Online via zoom.

[Handout](#)

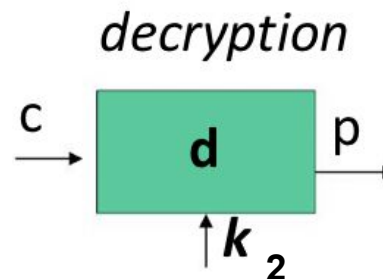
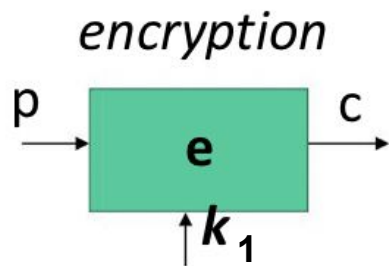
[Course Slides](#)

(1/3) Cryptography

What is a Cryptography?

- The science of **encrypting** and **decrypting** information is called **cryptography**.
- The result of encryption is **ciphertext** (c).
- We **decrypt** (d) ciphertext to recover plaintext.
- A **key** (k) is used to configure a cryptosystem.

$$p = d_{k_2}(e_{k_1}(p))$$



(2/3) Symmetric Key Cryptography

$$p = d_{k_2}(e_{k_1}(p))$$

- The two keys k_1 and k_2 are the same key k .

$$k_1 = k_2 = k$$

- Communicating parties share a secret key (k).

(3/3) Illustration of symmetric key cryptography

One-Time Pad: Encryption

a = 000 d = 001 e = 010 h = 011 i = 100 l = 101 o = 110 v = 111

Encryption: Plaintext \oplus Key = Ciphertext

	h	e	l	l	o	d	a	v	i	d
Plaintext:	011	010	101	101	110	001	000	111	100	001
Key:	111	101	110	101	111	100	000	101	110	000
Ciphertext:	100	111	011	000	001	101	000	010	010	001
	i	v	h	a	d	l	a	e	e	d

One-Time Pad: Decryption

a = 000 d = 001 e = 010 h = 011 i = 100 l = 101 o = 110 v = 111

Decryption: Ciphertext \oplus Key = Plaintext

	i	v	h	a	d	l	a	e	e	d
Ciphertext:	100	111	011	000	001	101	000	010	010	001
Key:	111	101	110	101	111	100	000	101	110	000
Plaintext:	011	010	101	101	110	001	000	111	100	001
	h	e	l	l	o	d	a	v	i	d



Thank You