10410CS 330500 Cryptography and Network Security

孫宏民 **Sun, Hung-Min**

一、課程說明(Course Description)

The course intends to provide a practical, up-to-date, and comprehensive survey of Cryptography and Network Security. This course will introduces the symmetric-key cryptography, both traditional and modern; asymmetric-key cryptography; hash function for message integrity and authentication; network security protocols.

二、指定用書(Text Books)

Forouzan, Behrouz A. ,Cryptography and Network Security, McGraw-Hall International Edition, 2008.

三、參考書籍(References)

1. Trappe, W., and Washington, L., Introduction to Cryptography and Coding. Upper Saddle River, NJ: Prentice Hall, 2006.
2. Stallings, W. Cryptography and Network Security. Upper Saddle River, NJ: Prentice Hall, 2006.
3. Schneier, B. Applied Cryptography, New York: Wiley, 1996.

四、教學方式(Teaching Method)

Lecturing

五、教學進度(Syllabus)

Introduction

Part One: Symmetric-Key Encipherment

(a) Mathematics of Cryptography
(b) Traditional Symmetric-Key Ciphers
(c) Modern Symmetric-Key Cipher
(d) DES
(e) AES

Part Two: Asymmetric-Key Encipherment

(a) Mathematics of Cryptography
(b) RSA, Rabin
(c) ElGamal

Part Three: Integrity, Authentication, and Key Management

(a) Message Integrity and Message Authentication
(b) Cryptographic Hash Functions
(c) Digital Signatures

(d) Entity Authentication

Part Four: Network Security

(a) Authentication Protocol

(b) Key management

六、成績考核(Evaluation)

Midterm I: 20%

Midterm II: 20%

Final Exam: 20%

Homeworks: 40%

Bonus: 5%

七、可連結之網頁位址

http://is.cs.nthu.edu.tw/course/2015Fall/CS330500/