

CCS4204 Computer System Security**COURSE INFORMATION**

Prerequisites	Academic Year & Level		Teaching Methods			Credit Hrs.
	Year	Semester	Lecture	Tutorial	Laboratory	
CCY2001 & CCS2001	4	8	2	2	0	3

COURSE AIM

- Identify threats and security attacks to computer systems.
- Master symmetric and asymmetric cryptography techniques.
- Experiment with symmetric and asymmetric key distribution protocols.
- Experiment with message authentication mechanisms.
- Experiment with system security.

COURSE WEEKLY CONTENTS

- 1 Introduction
- 2 Classical Encryption Techniques
- 3 Data Encryption Standards (DES)
- 4 Block cipher design principles/Block cipher modes of operation
- 5 Advanced encryption standard (AES)
- 6 Introduction to Number Theory
- 7 Public key cryptography
- 8 Key Distribution for Symmetric Encryption
- 9 Key Distribution for Asymmetric Encryption
- 10 Key Distribution for Asymmetric Encryption (cont.)
- 11 Message Authentication and Hash Functions
- 12 Digital Signatures
- 13 Firewalls
- 14 Intrusion Detection
- 15 Revision

STUDENT GRADING & ASSESSMENT

Weeks	Exams	Assign.	Quizzes	Reports	Present.	Lab.	Total
1 to 7	←		30	MARKS		→	30
8 to 12	←		20	MARKS		→	20
1 to 15	←		10	MARKS		→	10
16 or 17	40	Final					40

REFERENCES

Textbook W. Stallings, *Cryptography and Network Security, Principles and Practice*, Prentice Hall