

CCY4105 E-business Security**COURSE INFORMATION**

Prerequisites	Academic Year & Level		Teaching Methods			Credit Hrs.
	Year	Semester	Lecture	Tutorial	Laboratory	
CCY2001 & CIS1000	4	7/8	2	2	--	3

COURSE AIM

To get the students to:

- Understand related technologies in order to develop a secure e-commerce system
- Know the basic requirements for secure e-commerce systems
- Review areas of potential compromises in the security of client/server systems
- Analyze the vulnerabilities of a given system and make recommendations for making the system more secure.
- Develop an understanding of the client/server architecture and the various components used in distributed systems

COURSE WEEKLY CONTENTS

- 1 Course Aim, Course outline with an overview of e-Business and related security principles and concepts
- 2 Identification of common cyber threats targeting e-Businesses
- 3 Understanding basic web security models and protocols
- 4 Electronic Payment Systems and Payment Security Services
- 5 Electronic Payment Systems and Payment Security Services (cont.)
- 6 Principles of database security and data protection
- 7 7th week Assessment
- 8 Securing e-Business network architecture and protocols
- 9 Best practices for securing e-Business applications and platforms
- 10 Security challenges and solutions for mobile e-Business platforms
- 11 Securing cloud-based e-Business solutions and services
- 12 12th week Assessment
- 13 Regulatory compliance requirements and legal considerations
- 14 Strategies for detecting, responding to, and recovering from security incidents
- 15 Projects Presentations

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			Final Exam				40

REFERENCES

Textbook João Manuel R.S. Tavares et al. (Editors), Handbook of E-business Security, CRC press
Bryan Sullivan and Vincent Liu, Web Application Security, A Beginner's Guide, McGraw-Hill