

4.3.1.2.Cybersecurity Courses (CCY)

CCY3002 Introduction to Cryptography

COURSE INFORMATION

Prerequisites	Academic Year & Level		Teaching Methods			Credit Hrs.
	Year	Semester	Lecture	Tutorial	Laboratory	
CCY2001 and EBA2204	3	5	2	2	--	3

COURSE AIM

To get the students to:

- Understand cryptography principles and algorithms.
- Understand the design principles of symmetric and asymmetric ciphers
- Experiment with symmetric and asymmetric ciphers implementation and operation
- Understand cryptographic hash functions and message authentication codes
- Understand digital signatures algorithms and implementation
- Understand and experiment with key distribution protocols for symmetric and asymmetric cryptography

COURSE WEEKLY CONTENTS

- 1 Course Introduction and Syllabus discussion
- 2 Introduction to Number Theory
- 3 Classical Encryption Techniques
- 4 Block ciphers and the Data Encryption Standard
- 5 Finite Fields and Advanced Encryption standard
- 6 Block cipher operation
- 7 Random bit generation and stream ciphers
- 8 7th week Assessment
- 9 Public-key cryptography and RSA
- 10 Other Public Key cryptosystems
- 11 Cryptographic Hash functions and Message Authentication Codes
- 12 12th week Assessment and Digital Signatures
- 13 Cryptographic Key Management and Distribution
- 14 Cryptographic Key Management and Distribution (cont.)
- 15 Introduction to Quantum and Post-Quantum Cryptography

STUDENT GRADING & ASSESSMENT

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

REFERENCES

Textbook William Stallings, Cryptography and Network Security: Principles and Practice, Pearson
Jonathan Katz and Y. Lindell, Introduction to Modern Cryptography, CRC Press