CT-504	**:**	**Network Security**	**First Semester**
Text Book	**:**	Cryptography and Networking Security (International Edition) by Behrouz A. Forouzan	
Period	**:**	**45** periods for 15 weeks (3 periods/week) (Lecture + Lab)	

Course Description

This course unit aims to introduce the principles and practice of cryptography and network security. It covers cryptography, network-based security threats and vulnerabilities, and practical solutions to system and network security. It is designed for students who have some understanding of computer networks and protocols, but no background in security.

Course Objectives

Enable the students to learn fundamental concepts of computer security and cryptography and utilize these techniques in computing systems. This course unit covers security threats and vulnerabilities, principles of cryptography, and practical security solutions for networked and Internet environments.

References

1. Cryptography and Networking Security (International Edition) by Behrouz A. Forouzan
2. Applied Cryptography (Protocols, Algorithms, Source Code in C) by Bruce Schneief
3. Cryptography Decrypted by M. X. Mel Doris Baker
4. Network Security (2^nd Endition) by Charlie Kacfman, Radia Perlman, Mike Speciner

Assessment Plan for the Course

Paper Exam:	60%
Attendance:	10%
Test/ Quiz:	10%
Lab:	10%
Project:	10%

Tentative Lecture Plan

No.	Chapter	Page	Period	Detail Lecture Plan
	Chapter 11 **Message Integrity and Message Authentication**	339-362	**5**	All examples, review questions and Exercise
1.	11.1 Message Integrity	339-342	2	
2.	11.2 Random Oracle Model	343-351	2	
3.	11.3 Message Authentication	352-356	1	
	Chapter 12 **Cryptographic Hash Functions**	363-388	**5**	All examples, review questions and Exercises
4.	12.1 Introduction	363-366	2	
5.	12.2 SHA-512	367-375	2	
6.	12.3 Whirlpool	376-384	1	
	Chapter 13 **Digital Signature**	389-414	**6**	All examples, review questions and Exercises
7.	13.1 Comparison Modular Arithmetic 13.2 Process	390-392	1	
8.	13.3 Services	393-394	1	
9.	13.4 Attacks on Digital Signature	395-395	1	
10.	13.5 Digital Signature Scheme	396-408	2	
11.	13.6 Variations and Applications	409-411	1	
	Chapter 14 **Entity Authentication**	**415-436**	5	All examples, review questions and Exercises
12.	14.1 Introduction	415-416	1	
13.	14.2 Passwords	416-420	1	
14.	14.3 Challenge-Response	421-425	1	

15.	14.4 Zero-Knowledge 14.5 Biometrics	426-434	2	
	Chapter 15 **Key Management**	437-466	**5**	All examples, review questions and Exercises
17.	15.1 Symmetric-Key Distribution	438- 442	2	
18.	15.2 Kerberos	443 -447	1	
19.	15.3 Symmetric Key Agreement	447- 452	1	
20.	15.4 Public Key Distribution	453 -460	1	
	Chapter 16 **Security at the Application Layer: PGP and S/MIME**	467-506	**6**	All examples, review questions and Exercises
21.	16.1 E-Mail	467- 469	2	
22.	16.2 PGP	470- 492	2	
23.	16.3 S/MIME	492 -502	2	
	Chapter 17 **Security at the Transport Layer: SSL and TLS**	507-548	**5**	All examples, review questions and Exercises
24.	17.1 SSL Architecture	508- 516	2	
25.	17.2 Four Protocols	517–528	1	
26.	17.3 SSL Message Formats	529- 537	1	
27.	17.4 Transport Layer Security	538- 544	1	
	Chapter 18 **Security at the Network Layer: IPSec**	549-592	**6**	All examples, review questions and Exercises
28.	18.1 Two Modes	550-552	1	
29.	18.2 Two Security Protocols	552- 556	1	
30.	18.3 Security Association	557- 559	1	
31.	18.4 Security Policy	560 -560	1	
32.	18.5 Internet Key Exchange (IKE)	563 -577	1	
33	18.6 ISAKMP	578- 587	1	
34.	**Revision for All Chapters**		**2**	