University of Computer Studies, Yangon
B.C.Sc./B.C.Tech.

CT-405	**:**	**Cryptography**	**Second 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 focuses towards the introduction of network security using various cryptographic algorithms. Underlying network security applications.

Course Objectives:

- To lay a foundation on Security in Networks, Classical Cryptosystem and Block Cipher Modes of Operation, System Security, Malicious Softwares.
- To design various Private and Public key Cryptosystem for encryption, key exchange and hashing,
- To analyze various Private and Public key Cryptosystem for encryption and key exchange

Assessment Plan for the Course

Paper Exam: 60%

Attendance: 10%

Test/ Quiz: 10%

Lab: 10%

Lab Assessment: 10%

Tentative Lecture Plan

No.	Chapter	Page	Period	Detail Lecture Plan
1.	**Chapter 1 Introduction**		**3**	Overview
	Chapter 3 Traditional Symmetric Key Cipher	56-96	**12**	All review questions and problems

No.	Chapter	Page	Period	Detail Lecture Plan
2.	3.1 Introduction	56-61	2	
3.	3.2 Substitution Ciphers 3.3 Transposition Ciphers	61-80 80-87	8	
4.	3.4 Stream and Block Ciphers	87-96	2	
	Chapter 5 Introduction to Modern Symmetric Key Ciphers	124-158	**4**	Overview
6.	5.1 Modern Block Ciphers	124-148	2	
7.	5.2 Modern Stream Ciphers	148-158	2	
	Chapter 6 Data Encryption Standard (DES)	159-189	**7**	
8.	6.1 Introduction 6.2 DES Structure	159-160 160-175	5	All review questions, problems and Appendix O
9.	6.3 DES Analysis	175-181	2	
	Chapter 8 Encipherment Using Modern Symmetric-Key Ciphers	225-248	**7**	All review questions and problems
11.	8.1 Use of Modern Block Ciphers	225-238	2	
12.	8.2 Use of Modern Stream Ciphers Other Issues	238-244 244-248	5	
	Chapter 10 Asymmetric-Key Cryptography	293-335	**10**	
14.	10.1 Introduction 10.2 RSA Cryptosystem	293-300 301-314	4	All review questions and problems
15.	10.3 RABIN Cryptosystem	314-317	1	Overview
16.	10.4 ELGAMAL Cryptography	317	3	
17.	10.5 Elliptic Curve Cryptosystem	321-330	2	Overview
19.	Revision for All Chapters		**2**	

No.	Lab	Period (15)	Description
1.	Lab 1	2	▪ Caeser cipher ▪ Additive Cipher ▪ Multiplicative cipher
2.	Lab 2	1	Affine cipher
3.	Lab 3	2	▪ Playfair cipher ▪ Hill cipher
4.	Lab 4	1	Transposition Ciphers
5.	Discussion / Lab Review	1	
6.	Lab Assessment 1	1	

No.	Lab	Period (15)	Description
7.	Lab 5	1	Pseudo random number generation
8.	Lab 6	2	Symmetric Key Cryptography ▪ DES key creation ▪ Encryption and decryption with DES
9.	Lab 7	2	Asymmetric Key Cryptography ▪ RSA key pair generation ▪ Encryption and decryption with RSA
10.	Discussion / Lab Review	1	
11.	Lab Assessment 2	1	