FACULTY OF TECHNOLOGY & ENGINEERING
DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING

CS345: CRYPTOGRAPHY & NETWORK SECURITY

Credits and Hours:

Teaching Scheme	Theory	Practical	Tutorial	Total	Credit
Hours/week	4	2	-	6	5
Marks	100	50	-	150	

Outline of the Course:

Sr No.	Title of the unit	Minimum number of hours
1.	Classical Cryptography	**04**
2.	Shannon's Theory	**03**
3.	Block Ciphers And The Advanced Encryption Standard	**05**
4.	Cryptographic Hash Functions	**05**
5.	The RSA Cryptosystem And Factoring Integers	**05**
6.	Public-Key Cryptography And Discrete Logarithms	**05**
7.	Signature Schemes	**05**
8.	Pseudo-Random Number Generation	**03**
9.	Key Distribution & Key Agreement Schemes	**05**
10.	Public-Key Infrastructure & Multicast Security	**05**

Total hours (Theory): 60
Total hours (Lab): 30
Total hours: 90

Detailed Syllabus:

1.	**Classical Cryptography**	**04 hours**	**09 %**
1.1	Introduction: Some Simple Cryptosystems		
1.2	Cryptanalysis		
2.	**Shannon's Theory**	**03 hours**	**07 %**
2.1	Introduction		
2.2	Elementary Probability Theory		
2.3	Perfect Secrecy		
2.4	Entropy		
2.5	Product Cryptosystems		
3.	**Block Ciphers and The Advanced Encryption Standard**	**05 hours**	**11%**
3.1	Introduction		
3.2	Substitution-Permutation Networks		
3.3	The Data Encryption Standard		
3.4	The Advanced Encryption Standard		
3.5	Modes of Operation		
4.	**Cryptographic Hash Functions**	**05 hours**	**11%**
4.1	Hash Functions and Data Integrity		
4.2	Security of Hash Functions		
4.3	Iterated Hash Functions		
4.4	Message Authentication Codes		
5.	**The RSA Cryptosystem and Factoring Integers**	**05 hours**	**11%**
5.1	Introduction to Public-key Cryptography		
5.2	The RSA Cryptosystem		
5.3	Primality Testing		
5.4	Factoring Algorithms		
5.5	Other Attacks on RSA		
6.	**Public-Key Cryptography and Discrete Logarithms**	**05 hours**	**11%**
6.1	The ElGamal Cryptosystem		
6.2	Algorithms for the Discrete Logarithm Problem		
6.3	Lower Bounds on the Complexity of Generic Algorithms		
6.4	Finite Fields		
6.5	Elliptic Curves		

7.	**Signature Schemes**	**05 hours**	**11%**

7.1 Introduction
7.2 Security Requirements for Signature Schemes
7.3 The ElGamal Signature Scheme
7.4 Variants of the ElGamal Signature Scheme

8.	**Pseudo-Random Number Generation**	**03 hours**	**07%**

8.1 Introduction and Examples
8.2 The Blum-Blum-Shub Generator
8.3 Probabilistic Encryption

9.	**Key Distribution & Key Agreement Schemes**	**05 hours**	**11%**

9.1 Introduction
9.2 Diffie-Hellman Key Predistribution
9.3 Key Distribution Patterns
9.4 Session Key Distribution Schemes
9.5 Diffie-Hellman Key Agreement
9.6 Key Agreement Using Self-Certifying Keys
9.7 Encrypted Key Exchange

10.	**Public-Key Infrastructure&Multicast Security**	**05 hours**	**11%**

10.1 Introduction: What is a PKI?
10.2 Certificates
10.3 The Future of PKI?
10.4 Identity-Based Cryptography
10.5 Introduction to Multicast Security
10.6 Broadcast Encryption
10.7 Multicast Re-Keying

Course Outcome:

After completion of the course students will be able to

CO1	Define various security goal and understand the security policies such as the CIA triad of Confidentiality, Integrity and Availability.
CO2	Classify various forms of security attacks, where they arise, and appropriate tools or mechanism to quantify them.
CO3	Illustrate a basic understanding of cryptography, how it has evolved, and evaluate symmetric key encryption techniques used today.
CO4	Distinguish modern symmetric encryption standard, key distribution scenario and analyze effectiveness in todays' environment.
CO5	Evaluate Asymmetric key encryption techniques, key distribution scenario and calculate public and private components of asymmetric key encryption techniques.
CO6	Develop message integrity and message authentication of message digest.

Course Articulation Matrix:

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2
CO1	1	2	-	-	3	1	-	2	1	-	-	-	-	-
CO2	2	3	3	2	3	1	-	-	-	-	-	-	1	-
CO3	2	2	3	2	3	2	-	-	2	1	-	-	2	-
CO4	2	2	3	2	3	-	2	-	2	1	-	-	3	1
CO5	3	2	3	2	1	-	2	1	1	-	-	-	3	1
CO6	2	2	3	1	-	-	2	2	1	-	2	-	2	2

Recommended Study Material:

- **Text Books:**

1. Douglas R. Stinson, Cryptography: Theory and Practice, Chapman & Hall/CRC

- **Reference Books:**

1. William Stallings, Cryptography And Network Principles And Practice,Prentice Hall, Pearson Education Asia
2. AtulKahate, Cryptography & Network Security, The McGraw-Hill Companies
3. Behrouz A. Forouzan, Cryptography and Network Security, McGraw-Hill Companies

- **Reference Links/ e-content:**

1. http://people.csail.mit.edu/rivest/crypto-security.html
2. http://www.cryptix.org/
3. http://www.cryptocd.org/
4. http://www.cryptopp.com/