### **CS361: CRYPTOGRAPHY & NETWORK SECURITY**

### **Credits and Hours:**

Teaching Scheme	Theory	Practical	Tutorial	Total	Credit
Hours/week	3	2	-	6	4
Marks	100	50	-	150	

## A. Pre-requisite Course:

- Data Communication and Networking
- Engineering Mathematics

### **B.** Outline of the Course:

Sr	Title of the unit	Minimum number of hours			
No.					
1.	Classical Cryptography	6			
2.	Block Ciphers And The Advanced Encryption Standard	6			
3.	Cryptographic Hash Functions	5			
4.	The RSA Cryptosystem And Factoring Integers	8			
5.	Signature Schemes	8			
6.	Key Distribution & Key Agreement Schemes	12			

Total hours (Theory): 45 Total hours (Lab): 30 Total hours:65

# C. Detailed Syllabus:

1.	Classical Cryptography	06 hours	12 %
1.1 1.2	Introduction: Some Simple Cryptosystems Cryptanalysis		
1.3 1.4	Introduction to Shannon's Theory Elementary Probability Theory		
1.5	Perfect Secrecy		
1.6	Entropy		
1.7	Product Cryptosystems		
2.	<b>Block Ciphers And The Advanced Encryption Standard</b>	06 hours	13%
2.1 2.2 2.3 2.4 2.5	Introduction Substitution-Permutation Networks The Data Encryption Standard The Advanced Encryption Standard Modes of Operation		
3.	Cryptographic Hash Functions	05 hours	13%
3.1 3.2 3.3 3.4	Hash Functions and Data Integrity Security of Hash Functions Iterated Hash Functions Message Authentication Codes		
4.	The RSA Cryptosystem And Factoring Integers	08 hours	17%
4.1 4.2 4.3 4.4 4.5	Introduction to Public-key Cryptography The RSA Cryptosystem, The ElGamal Cryptosystem Primality Testing Factoring Algorithms Other Attacks on RSA		

### 5. Signature Schemes

- 5.1 Introduction
- 5.2 Security Requirements for Signature Schemes
- 5.3 The ElGamal Signature Scheme
- 5.4 Variants of the ElGamal Signature Scheme
- 5.5 Pseudo-Random Number Generation- Introduction and

#### Examples

- 5.6 The Blum-Blum-Shub Generator
- 5.7 Probabilistic Encryption

### 6. Key Distribution & Key Agreement Schemes

12 hours 29%

- 6.1 Introductio n
- 6.2 Diffie-Hellman Key Predistribution
- 6.3 Key Distribution Patterns
- 6.4 Session Key Distribution Schemes
- 6.5 Diffie-Hellman Key Agreement
- 6.6 Key Agreement Using Self-Certifying Keys
- 6.7 Encrypted Key Exchange
- 6.8 Introduction to PKI and Multicast Security:
- 6.9 What is a PKI, Certificates
- 6.10 The Future of PKI?
- 6.11 Identity-Based Cryptography
- 6.12 Introduction to Multicast Security
- 6.13 Broadcast Encryption
- 6.14 Multicast Re-Keying

### D. Instructional Method and Pedagogy:

- At the start of course, the course delivery pattern, prerequisite of the subject will be discussed.
- Lectures will be conducted with the aid of multi-media projector, black board, OHP etc.
- Attendance is compulsory in lectures and laboratory which carries 5 Marks weightage.
- Two internal exams will be conducted and average of the same will be converted to equivalent of 15 Marks as a part of internal theory evaluation.

8 hours 16%

- Assignments based on course content will be given to the students at the end of each unit/topic and will be evaluated at regular interval. It carries a weightage of5Marksas a part of internal theory evaluation.
- Surprise tests/Quizzes/Seminar will be conducted which carries 5 Marks as a part of internal theory evaluation.
- The course includes a laboratory, where students have an opportunity to build an appreciation for the concepts being taught in lectures.
- Experiments/Tutorials related to course content will be carried out in the laboratory.

#### E. Course Outcomes:

After completion of the course, Students will be able to:

CO1	Classify various security goals, mechanisms and attacks.
CO2	Evaluate symmetric and asymmetric key encryption techniques.
CO3	Implement the security mechanisms on given environment (scenario).
CO4	Design the technique or model to provide security for given scenario.
CO5	Practically work on various network security applications, IPsec, Firewall, IDS, Web security, Email security, and malicious software etc.
CO6	Perform simple vulnerability assessments and password audits and also able to configure simple firewall architectures and Understand Virtual Private Networks

### F. Course Articulation Matrix

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

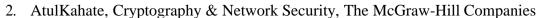
### G. Recommended Study Material:

#### **\*** 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



3. Behrouz A. Forouzan, Cryptography and Network Security, McGraw-Hill Companies

### **\*** Web Materials:

- 1. http://people.csail.mit.edu/rivest/crypto-security.html
- 2. <a href="http://www.cryptix.org/">http://www.cryptix.org/</a>
- 3. <a href="http://www.cryptocd.org/">http://www.cryptocd.org/</a>
- 4. <a href="http://www.cryptopp.com/">http://www.cryptopp.com/</a>