Course Title: Introduction to Cryptography **Credit: 3**
Course No: CSIT.321 **Number of period per week: 3+3**
Nature of the Course: Theory + Lab **Total hours: 45+45**
Year: Third, Semester: Sixth
Level: B. Sc. CSIT

1. Course Introduction

Cryptography provides important tools for ensuring the privacy, authenticity, and integrity of the increasingly sensitive information involved in modern digital systems. Nowadays, core cryptographic tools, including encryption, message authentication codes, digital signature, key agreement protocols, etc., are used behind millions of daily on-line transactions. This course will unveil some of the magic of cryptography.

2. Objectives

By the end of this course, students will be able to

- → Understand different cryptographic schemes their goals and limitations
- → Explain how security systems works and how these systems can be attacked by imposters
- → Demonstrate and implement different cryptographic algorithms and protocols
- → Analyze strength of implemented sedulity mechanisms

3. Specific Objectives and Contents

Specific Objectives	Contents
• Understand need and importance of cryptography • Discuss security attacks, services and mechanism • Demonstrate classical cipher techniques	**Unit I: Introduction & Classical Encryption (8 hr Hrs)** 1.1. Defining Cryptography and Cryptanalysis, Security Attacks, Security Services, Security Mechanisms 1.2. Virus, Worms, Torjan Horse, Types of Crypto Systems and their comparison, Symmetric cipher model 1.3. Substitution Techniques: Caeser, Monoalphabetic, Playfair, Hill, Polyalphabetic ciphers, one-time pad 1.4. Transposition Techniques, Steganography, Overview of Shannon's Theory, Block ciphers vs Stream Ciphers
• Understand working of symmetric ciphers • Discuss mathematical concepts used in symmetric ciphers • Exemplify different symmetric ciphers and implement them	**Unit II: Modern Symmetric Ciphers (10 hr)** 2.1. Block Cipher Principles, Data Encryption Standards, Strength of DES 2.2. Finite Fields: Groups Rings, Fields, Modular Arithmetic, Euclidean Algorithm, Galois Fields (GF(p) & GF(2^n)), Polynomial Arithmetic 2.3. AES (Advanced Encryption Standards) Cipher, AES Evaluation 2.4. Double DES, Triple DES, Stream Cipher Structure, RC4 Algorithm

• Discuss Number Theory that is useful in asymmetric ciphers • Demonstrate different asymmetric ciphers • Understand different types of attacks on symmetric ciphers • Implement asymmetric cipher techniques	**Unit III: Asymmetric Ciphers (10 hr)** 3.1. Number Theory: Prime Numbers, Fermats Theorem, Euler Theorem, Primility Testing, Chinese Remainder Theorem, Discrete Logarithms 3.2. Public Key Cryptosystems, Applications of Public Key Cryptosystems, Requirements of Public Key Cryptosystems, Public Key Cryptanalysis 3.3. RSA Algorithm, Computational aspects of RSA, Security of RSA 3.4. Distribution of public key, Distribution of secret key by using public key cryptography, Diffie-Helman Key Exchange and Man-in-the-Middle Attack, Elliptic Curve Arithmetic, Elliptic Curve Cryptography, The ElGamal Encryption Algorithm
• Understand hashing and hash value • Demonstrate hashing algorithms to generate hash value • Understand attacks on hash functions	**Unit IV: Hashing (6 hr)** 4.1. Authentication Requirements, Authentication Functions, Message Authentication Codes 4.2. Hash Functions and Birthday Attacks, Security of Hash Functions and MACs, Message Digests (MD5) 4.3. Secure Hash Algorithm (SHA-512), HMAC, Security of HMAC, CMAC
• Understand role and operation of digital signatures • Discuss different authentication protocols • Explain digital signature standard and DS algorithm	**Unit V: Digital Signatures and Authentication (6 Hrs)** 5.1. Digital Signatures: Direct Digital Signatures, Arbitrated Digital Signature 5.2. Authentication Protocols: Mutual Authentication, One-way Authentication 5.3. Digital Signature Standard: The DSS Approach, Digital Signature Algorithm
• Discuss different protocols used in authentication • Demonstrate PGP used in email security • Understand role and working of SSL, TLS and SET • Explain intruders and intrusion detection techniques	**Unit VI: Network Security (6 Hrs)** 6.1. Authentication Applications: Kerberos, Public Key Infrastructure 6.2. Email Security: Pretty Good Privacy (Description, Keys, Key Management) 6.3. IP Security, Web Security, Secure Socket Layer, Transport Layer Security Secure Electronic Transaction, Dual Signature, Payment Processing 6.4. Intruders, Intrusion Detection (Statistical Anaomaly Detection, Rule Based Intruder Detection), Password Protection, Password Selection, Firewalls

Evaluation System

Undergraduate Programs							
External Evaluation	**Marks**	**Internal Evaluation**	**Weightage**	**Marks**	**Practical**	**Weightage**	**Mark**
End semester examination	60	Assignments	20%	20	Practical Report copy	25%	20
(Details are given in the separate table at the end)		Quizzes	10%		Viva	25%	
		Attendance	20%		Practical Exam	50%	
		Internal Exams	50%				
Total External	60	Total Internal	100%	20		100%	20
Full Marks 60+20+20 = 100							

External evaluation

1. **End semester examination:**
   It is a written examination at the end of the semester. The questions will be asked covering all the units of the course. The question model, full marks, time and others will be as per the following grid.

2. **External Practical Evaluation:**
   After completing the end semester theoretical examination, practical examination will be held. External examiner will conduct the practical examination according to the above mentioned evaluation. There will be an internal examiner to assist the external examiner. Three hours time will be given for the practical examination. In this examination Students must demonstrate the knowledge of the subject matter.

Full Marks: 100, Pass Marks: 45, Time: 3 Hrs

Nature of question	Total questions to be asked	Total questions to be answered	Total marks	Weightage
Group A: multiple choice*	20	20	20×1 = 20	60%
Group B: Short answer type questions	7	6	6×8 = 48	60%
Group C: Long answer type questions	3	2	2×16 =32	60%
			100	100%

Each student must secure at least 50% marks in internal evaluation in order to appear in the end semester examination. Failed student will not be eligible to appear in the end semester examinations.

Internal evaluation

Assignment: Each student must submit the assignment individually. The stipulated time for submission of the assignment will be seriously taken.

Quizzes: Unannounced and announced quizzes/tests will be taken by the respective subject teachers. Such quizzes/tests will be conducted twice per semester. The students will be evaluated accordingly.

Attendance in class: Students should regularly attend and participate in class discussion. Eighty percent class attendance is mandatory for the students to enable them to appear in the end semester examination. Below 80% attendance in the class will signify NOT QUALIFIED (NQ) to attend the end semester examination.

Presentation: Students will be divided into groups and each group will be provided with a topic for presentation. It will be evaluated individually as well as group-wise. Individual students have to make presentations on the given topics.

Mid-term examination: It is a written examination and the questions will be asked covering all the topics in the session of the course.

Discussion and participation: Students will be evaluated on the basis of their active participation in the classroom discussions.

Instructional Techniques: All topics are discussed with emphasis on real-world application. List of instructional techniques is as follows:

- Lecture and Discussion
- Group work and Individual work
- Assignments
- Presentation by Students
- Quizzes
- Guest Lecture

Students are advised to attend all the classes and complete all the assignments within the specified time period. If a student does not attend the class (es), it is his/her sole responsibility to cover the topic(s) taught during that period. If a student fails to attend a formal exam/quiz/test, there won't be any provision for re-exam. Unless and until the student clears one semester he/she will not be allowed to study in the following semesters.

Laboratory Work

Student should write programs and prepare lab sheet for all of the units in the syllabus. Students should be able to implement different cryptographic algorithms discussed in class. The lab work should be practiced for minimum of 3 lab hours per week.

Prescribed Text

- W. Stallings, "Cryptography and Network Security", Pearson Education.

References

- Douglas Stinson, "Cryptography Theory and Practice", 2nd Edition, Chapman & Hall/CRC.
- B. A. Forouzan, "Cryptography & Network Security", Tata Mc Graw Hill.