Course Title: Cryptography **Full Marks: 60+20+20**
Course No: CSC316 **Pass Marks: 24+8+8**
Nature of the Course: Theory + Lab **Credit Hours: 3**
Year/Semester: Third/Fifth

Course Description: The course introduces the underlying the principles and design of cryptosystems. The course covers the basics concepts of cryptography including: traditional ciphers, block ciphers, stream ciphers, public and private key cryptosystems. The course also includes the theory of hash functions, authentication systems, network security protocols and malicious logic.

Course Objectives: The objectives of this course are to familiarize the students with cryptography and its applications. The students will be able to develop basic understanding of cryptographic mechanisms.

Detail Syllabus

Chapters / Units	Teaching Methodology	Teaching Hours
Unit I: Introduction and Classical Ciphers 1.1. Security: Computer Security, Information Security, Network Security, CIA Triad: Confidentiality, Integrity, Availability, Cryptography, Cryptosystem, Cryptanalysis, Security Threats:, Attacks: Passive (Release of message, Traffic analysis), Active (Replay, Denial of service) Security Services: Authentication, Access Control, Nonrepudiation Security Mechanisms, Policy and Mechanism 1.2. Classical Cryptosystems: Hierarchy of cipher Substitution Techniques: - Monoalphabetic: Ceasar Cipher, Hill - Polyalphabetic: Vigenere Cipher (Variants: vernam, one time pad), Playfair Transposition Techniques: Rail Fence Cipher 1.3. Modern Ciphers: Block Ciphers, Stream Ciphers,Symmetric Ciphers, Asymmetric Ciphers	**Class Lecture** **+** **Lab Session**	**7 Hours**

Unit II: Symmetric Ciphers 2.1. Fiestel Cipher Structure, Substitution Permutation Network (SPN) 2.2. Data Encryption Standards (DES): Key Generation, Encryption and Decryption Process, Weak Keys in DES, Double DES, Meet in Middle Attack, Triple DES 2.3. Finite Fields: Basic concepts of Groups, Rings, and Fields, GCD, Euclidean Algorithm, Modular Arithmetic, Set of Residue (Zn), Congruence, Residue classes, Quadratic residue, Operations on Zn (Addition, Subtraction, Multiplication), Properties of Zn, Inverses: Additive Inverse, Multiplicative Inverse, Relatively Prime, Extended Euclidean Algorithm, Galois Fields (GF(p) & GF(2^n)), Polynomial Arithmetic : Addition, Multiplication and Division over Galois Field 2.4. International Data Encryption Standard (IDEA): Key Generation, Encryption and Decryption Process 2.5. Advanced Encryption Standards (AES): Key Generation, Encryption and Decryption Process 2.6. Modes of Block Cipher Encryptions (Electronic Code Book, Cipher Block Chaining, Cipher Feedback Mode, Output Feedback Mode, Counter Mode)	**Class Lecture** **+** **Lab Session**	**10Hours**
Unit III: Asymmetric Ciphers 3.1. Number Theory: Prime Numbers, Primality Testing, Miller-Rabin Algorithm,Fermat's Theorem, Euler's Totient Function andEuler's Theorem, Primitive Root, Discrete Logarithms 3.2. Public Key Cryptosystems, Applications of Public Key Cryptosystems 3.3. Distribution of public key, Distribution of secret key by using public key cryptography, Diffie-Hellman Key Exchange, Man-in-the-Middle Attack 3.4. RSA Algorithm: Key Generation, Encryption and Decryption Process	**Class Lecture** **+** **Lab Session**	**8 Hours**

3.5. Elgamal Cryptographic System: Key Generation, Encryption and Decryption Process		
Unit IV: Cryptographic Hash Functions and Digital Signatures 4.1. Message Authentication, Message Authentication Functions, Message Authentication Codes 4.2. Hash Functions, Properties of Hash functions, Applications of Hash Functions 4.3. Message Digests: Details of MD4 and MD5 algorithms 4.4. Secure Hash Algorithms: Details of SHA-1 and SHA-2 algorithms, Comparison of SHA parameters, SHA-512 4.5. Digital Signatures: Direct Digital Signatures, Arbitrated Digital Signature 4.6. Digital Signature Standard: The DSS Approach, Digital Signature Algorithm(DSA) 4.7. Digital Signature Standard: The RSA Approach	**Class Lecture** **+** **Lab Session**	**8Hours**
Unit V: Authentication 5.1. Authentication System, 5.2. Password Based Authentication, Dictionary Attacks (Online and Offline), 5.3. Challenge Response System, One Way Authentication, Mutual Authentication 5.4. Biometric System 5.5. Needham-Schroeder Scheme, Kerberos Protocol, Kerberos 5	**Class Lecture** **+** **Lab Session**	**3 Hours**

Unit VI: Network Security and Public Key Infrastructure 6.1. Overview of Network Security 6.2. Digital Certificates and X.509 certificates, Certificate Life Cycle Management 6.3. PKI trust models, PKIX 6.4. Email Security: Pretty Good Privacy (PGP), Services provided by PGP 6.5. Secure Socket Layer (SSL) Protocol 6.6. Transport Layer Security (TLS) Protocol 6.7. IP Security (IPSec) Protocol 6.8. Firewalls, Firewall Characteristics, Types of Firewalls: Packet filtering firewall, Circuit-level gateway, Stateful inspection firewall, Proxy firewall, Next-generation firewall	**Class Lecture** **+** **Lab Session**	**6 Hours**
Unit VII: Malicious Logic (3 Hrs) 7.1.Malicious Logic, Types of Malicious Logic: Virus, Worm, Trojan Horse, Zombies, Denial of Service Attacks, 7.2. Intrusion, Intruders and their types (Masquerader, Misfeasor, Clandestine),Intrusion Detection System: Statisticalanomaly detection, Rule-based detection	**Class Lecture** **+** **Lab Session**	**6 Hours**

Text Book:

1. W. Stallings, *Cryptography and Network Security: Principles and Practice*

Reference Books:

1. William Stallings, *Network Security Essentials: Applications and Standards*
2. Matt Bishop, *Computer Security, Art and Science*.
3. Mark Stamp, *Information Security: Principles and Practices.*
4. Bruce Schneier, *Applied Cryptography*.
5. Douglas. R. Stinson. *Cryptography: Theory and Practice.*
6. B. A. Forouzan, *Cryptography & Network Security*, Tata Mc Graw Hill.

Laboratory Work Manual

Student should write programs and prepare lab sheet for all of theunits in the syllabus. Students should implement cryptographic algorithmsand protocols mentioned in each. The choice of programming language can be decided by the instructor and student as per their comfort. The instructors have to prepare lab sheets for individual units covering the concept of the units as per the requirement. All of the lab reports should be evaluated during the corresponding weeks of hands on practice. The lab session for above chapters should be as per following description however the depth of lab works are not limited to the below mentioned contents only. The lab report might cover the following list of the programs.

Write the program to illustrate the followings

- Monoalphabetic Ciphers: Ceasar, Hill
- Polyalphabetic Cipher: Vigenere Cipher (Vernam, OTP), Playfair
- Transposition Cipher: Rail Fence Cipher
- Some basic components of DES like functioning of S-Box, Key generation
- Modular Arithmetic (Finding additive inverse, multiplicative inverse (Extended Euclidean algorithm, relatively prime)
- Number Theory (Primality testing, Totient function, Primitive root)
- Diffie-Helman Key Exchange, RSA Algorithm, Elgamal Cryptographic System
- Some basic logic for Malicious code

Model Question
Tribhuvan University
Institute of Science and Technology

Course Title: Cryptography **Full Marks:** 60
Course No: CSC316 **Pass Marks:** 24
Level: B. Sc CSIT Third Year/ Fifth Semester **Time: 3 Hrs**

Section A
Long Answer Questions

*Attempt any **TWO** questions.* *[2×10=20]*

1. Mention the families SHA-2? Describe how 160-bit of hash value is generated by taking an input message of variable size using SHA-1? [2+8]
2. Discuss how encryption and decryption is done using RSA? In a RSA system, a user Named Ram has chosen the primes 5 and 7 to create a key pair. The public key is (e_{Ram},n) and the private key is (d_{Ram}, n). Compute the private and public key pairs. Suppose another user Sita knows public key of Ram and want to send the plaintext "hi" to Ram using RSA Scheme. Show how Sita has encrypted the plaintext and Ram has decrypted the ciphertext. [5+5]
3. Describe the working principle of Fiestel Cipher Structure.Give the encryption and decryption procedure for 2-DES and 3-DES. Find the multiplicative inverse of 7 in Z_{11} using Extended Euclidean Algorithm. [4+2+4]

Section B
Short Answer Questions

*Attempt any **EIGHT** questions.* *[8×5=40]*

4. Define authentication system. How challenge response systems can be used as authentication approach? [1+4]
5. Define SSL. How SSL Record Protocol provides security in Secure Socket Layer Protocol? [1+4]
6. Decrypt the message "CMAL" using the Hill cipher with the key $\begin{pmatrix} 7 & 8 \\ 11 & 11 \end{pmatrix}$. Show your calculations and the result.
7. Divide $5x^2 + 4x + 6$ by $2x + 1$ over GF(7). [5]
8. Differentiate between virus, worm and trojan horse. [5]
9. Describe the purpose of PKI trust model? List any four types of firewall. [3 + 2]
10. What is digital signature? How DSS Approach is used to generate digital signature? [1+4]
11. Define Euler totient function. Find out whether 3 is primitive root of 7? [1 + 4]
12. Write Short Notes On (Any ***TWO***) [2.5 + 2.5]
    a. Vernam Cipher
    b. Kerberos Protocol
    c. Intrusion Detection System