DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
KATHMANDU UNIVERSITY

Subject: Information Security **Course Code: COMP 485**
Credit: 3 **F.M: 100**
Type: Elective

Course Description

This course introduces the role of cryptography in Computer Science. This will enable students to get broad knowledge on the key concepts like authentication, key distribution, access control etc. and also outlines the counter measure in the event of attacks.

Course Objectives

The course aims to:

1. Clarify the concept of information security, privacy and related concepts;
2. Describe threats to information security and how they can be addressed;
3. Provide an overview of standards of information security and privacy protection that are being applied

Prerequisite:

1. Calculus
2. Programming skills
3. Computer Networks
4. Database concepts

Evaluation:

Internal: 50

Final**:** 50

Contents:

Unit 1: Introduction to Information Security [2 hrs]

1.1 Introduction
1.2 The need of Security
1.3 Security Approaches
1.4 Principle of Security
1.5 Types of attacks

Unit 2: Symmetric Key Cryptographic methods [3 hrs]

2.1 Introduction to Symmetric Key Cryptography

2.2 Revision to Data Encryption Standard

2.3 Revision to Advanced Encryption Standard

2.4 RC4 and RC5

2.5 Blowfish

Case Study: Secure Multiparty Calculations

Unit 3: Asymmetric Key Cryptographic methods [10 hrs]

3.1 Introduction to Asymmetric Key Cryptography

3.2 ElGamal Cryptography

3.3 Digital Signature

3.4 Knapsack Algorithm

3.5 ElGamal Digital Signature

3.6 Threats on Digital Signature

Case Study: Contract Signing

Case Study: Virtual Elections

Unit 4 Public Key Infrastructure [6 hrs]

4.1 Introduction to PKI

4.2 Digital Certificates

4.3 Key Management

4.4 The PKIX model

4.5 XML, PKI and Security

Case Study: Cross Site Scripting Vulnerability

Unit 5 Internet Security Protocols [8 hrs]

5.1 Introduction to Internet Security Protocols

5.2 Secure Socket Layer(SSL)

5.3 Transport Layer Security(TLS)

5.4 Secure Electronic Transactions(SET)

5.5 Email Security

5.6 Wireless Application Protocol (WAP) security

Case Study: Secure Inter-branch Payment Transactions

Case Study: Cookies and Privacy

Unit 6 User Authentication Mechanism [10 hrs]

6.1 Introduction to Authentication

6.2 Generating Strong Passwords and Tokens

6.3 Certificate based Authentication

6.4 Biometric Authentication

6.5 Kerberos

6.6 Key Distribution Center (KDC)

6.7 Attacks in Authentication Schemes

Case Study: Single Sign On

Unit 7 Network Security, Firewalls and Virtual Private Networks [6 hrs]

7.1 Introduction to Network Security

7.2 Review of TCP/IP protocol

7.3 Firewalls

7.4 IP security

7.5 Virtual Private Networks

7.6 Intrusion detection and prevention

Case Study: IP spoofing attacks

Case Study: Creating a VPN

Practical:

- Discussion of Case studies and its solutions
- Implementation of symmetric and asymmetric encryption techniques

- Tools to monitor attacks and methods of prevention
- Use of Kali Linux and metasploit for penetration testing/vulnerability assessment
- Configuring a Linux-based packet-filtering firewalls using various methods

Text / Reference books :

1. D. R. Stinson. *Cryptography: Theory and Practice.* CRC Press
2. William Stallings, *Network Security Essentials-Applications & Standards*, Pearson.
3. Charlie Kaufman, Radia Perlman, Mike Speciner, *Network Security Private Communication in a Public World*, Second Edition, 2004 ,Pearson.
4. Matt Bishop, *Computer Security, Art and Science*, Pearson
5. Bruce Schneier, *Applied Cryptography*, Pearson
6. Atul Kahate, Cryptography and Network Security, 3e, McGraw Hill Education