Pokhara University
Faculty of Science and Technology

Course Code.: **CMP 426** (3 Credits) Full marks: **100**
Course title: **Network and Cyber Security (3-1-2)** Pass marks: **45**
Nature of the course: **Theory, Tutorial & Practical** Time per period: **1 hour**
Year, Semester: **Year 4, Sem 7th** Total periods: **45**
Level: **Bachelor** Program: **BECE**

1. Course Description

This course is about information security - cryptographic algorithms and their mathematical foundations. This course pays special attention to web (cyber) security and its standards and practices. Network security scenarios, standards and practices will also be studied along with their practical implications.

2. General Objectives

The general objectives of the course are: -

- to impart fundamental understanding of cryptographic algorithms and protocols
- to make students understand about the authentication and public key infrastructure
- to develop skills on the secure web, email services and emerging cyber security tools

3. Contents in Detail

Specific Objectives	Contents
To learn about the standard terms and models used in network security	**Unit I: Introduction to Network Security (3 hours)** 1.1 Security, Attack, Types of Attack 1.1.1 Virus, Worm, Trojan Horse 1.1.2 Intruder, Hacker, Role of Firewall and DMZ 1.2 CIA Triad, Security Service, Security Mechanism 1.3 Network Security Model, Network Security Access Model
To understand about the conventional cryptography, symmetric key cryptography and block cipher	**Unit II: Symmetric Key Cryptography (9 hours)** 2.1 Cryptology, Cryptography, Cryptanalysis 2.2 Conventional Cryptography, Single Key Encryption, Computationally Secure Algorithm 2.3 Stream Cipher, Substitution and Transposition Cipher 2.4 Block Cipher, Feistel Cipher Structure 2.4.1 Data Encryption Standard (DES), 2DES, 3DES 2.4.2 Advanced Encryption Standard (AES)
To understand about public cryptography, and its various encryption schemes.	**Unit III: Asymmetric Key Cryptography (9 hours)** 3.1 Need of Public Key, Asymmetric Cipher Model, 3.2 Prime Factorization Problem, RSA Encryption 3.3 Discrete Logarithm Problem, 3.3.1 Diffie – Hellman Key Exchange, 3.3.2 ElGamal Encryption

	3.3.3 Elliptic Curve Cryptography
To know about the authentication system and key establishment problems in both symmetric and asymmetric cryptography	**Unit IV: Authentication System and Key Establishment (9 hours)** 4.1 Hash, Secure Hash Algorithm (SHA) 4.2 Authentication in Symmetric Key Cryptography 4.2.1 Message Authentication Code (MAC), 4.2.2 Message Digest (MD), 4.2.3 HMAC - Prefix, Suffix and Nested 4.3 Authentication in Asymmetric Key Cryptography 4.3.1 Digital Signature 4.3.2 RSA Digital Signature 4.3.3 Digital Signature Standard 4.4 Key Establishment 4.4.1 n^2 Key Distribution Problem 4.4.2 Key Distribution Centre 4.4.3 Man-In-the-Middle (MIM) Attack 4.4.4 Digital Certificate
To have an in-depth understanding about cyber security including ssl, email and various web-related security standards.	**Unit V: Cyber (Web) Security (9 hours)** 5.1 Approaches to Web Security 5.2 Secure Socket Layer Architecture, Transport Layer Security 5.3 IPSec 5.3.1 IPSec Transport Mode 5.3.2 IPSec Tunnel Mode 5.4 Email Security 5.4.1 Pretty Good Privacy 5.4.2 S/MIME
To enable students to learn about the IT industry's security standard and practices about web application development.	**Unit VI: Web Application Security: Standards and Practices (6 hours)** 6.1 OWASP Top 10 6.2 Ways to maintain Security 6.2.1 Authentication and Authorization, 6.2.2 Data Protection in Storage and Transit, Data Validation and Parameter Validation 6.2.3 Error Handling and Exception Management 6.2.4 User and Session Management 6.2.5 Auditing and Logging 6.3 Security Testing 6.3.1 Broken Access Control 6.3.2 Various failures - Cryptographic Failures, Identification and Authentication Failures, Software & Data Integrity Failures, Security Loggin and Monitoring Failures

	6.3.3 Various types of Injection - XSS, Command Injection, LDAP Injection, XML Injection, Server-side Template Injection 6.3.4 Insecure Design, Vulnerable & Outdated Components 6.3.5 Server-Side Request Forgery (SSRF) – Input Validation, Whitelisting, Firewall Rules, User of Safe APIs, Least Privilege

4. Methods of Instruction

The main method of instruction is lecture delivery followed by tutorial classes of cryptographic algorithms and their mathematical foundation. Practical classes / lab works are conducted for every unit wherever possible. *{see section 6 for the list of practical works.}*

5. List of Tutorials (*Not all are mandatory, selective ones may be done. Tutorial class may also be conducted by invited experts from the industry.***)**

S.N.	Tutorials (T)
1	***For Unit II,*** T2.1 Modular Arithmetic and Closure Property, T2.2 Use of Prime Numbers in Encryption and Decryption, T2.3 Greatest Common Divisor, Inversion, Euclid's Algorithm and Extended Euclid's Algorithm T2.4 Finite Fields and Galois Field with Polynomial Equation
2	***For Unit III,*** T3.1 Relative Prime Number and Euler's Totient Function T3.2 Discrete Logarithm, Cyclic Group T3.3 Elliptic Curve Discrete Logarithm
3	***For Unit IV,*** T4.1 Padding Schemes in Hashing Algorithms T4.2 Collision Detection in Hashes T4.3 Key Distribution in Kerberos
4	***For Unit V,*** T5.1 IPSec Internet Key Exchange and Security Association T5.2 Packet Capturing and Analysis T5.3 RFC standards for Internet Email and MIME extensions
5	***For Unit VI,*** T6.1 Underlying concepts of the techniques mentioned in the unit.

6. **Practical Works (***Not all are mandatory, selective ones may be done. Practical work may also be replaced with case study, where students shall analyze the existing implementation of the assigned practical work.***)**

S.N.	Practical work / Case study (P)
1	***For Unit II,*** P2.1 Implement Caesar cipher and/or any mono-alphabetic cipher in any platform.

	P2.2 Implement Playfair and/or any multi-gram substitution cipher by using a suitable tool. P2.3 Implement Rail Fence and/or Vigenère cipher in a suitable platform. P2.4 Implement Vernam cipher and/or One-Time Pad algorithm. P2.5 Develop 3DES and/or AES cipher suite using suitable tools and in any platform.
2	***For Unit III,*** P3.1 Implement RSA key generation algorithm. P3.2 Develop RSA encryption and decryption scheme. P3.3 Make DHKE protocol and use it in the product developed in P2.5 P3.4 Develop ElGamal cipher by using the DHKE developed in P3.3 and by implementing a masking algorithm.
3	***For Unit IV,*** P4.1 Implement MAC and HMAC in Symmetric Key Cryptography. P4.2 Develop RSA digital signature and verify it. P4.3 Create a digital signature using DSS and verify it. P4.4 Demonstrate a MIM attack in your controlled environment.
4	***For Unit V,*** P5.1 Obtain a free SSL for email and try exchanging messages in your group. P5.2 Obtain PGP tools like GPG, OpenPGP etc. and implement it on your email clients and try exchanging messages in your group.
5	***For Unit VI,*** P6.1 Testing using NMAP tool, Burp suite etc.

7. Evaluation System and Students' Responsibilities

Evaluation System

In addition to the formal exam(s) conducted by the Office of the Controller of Examination of Pokhara University, the internal evaluation of a student may consist of class attendance, class participation, quizzes, assignments, presentations, written exams, etc. The tabular presentation of the evaluation system is as follows.

External Evaluation	**Marks**	**Internal Evaluation**	**Marks**
Semester-End Examination	50	Class attendance and participation	5
		Practical	20
		Assignments and presentations	5
		Internal Term Exam	20
Total External	50	Total Internal	50
Full Marks 50+50=100			

Students' Responsibilities:

Each student must secure at least 45% marks in the internal evaluation with 80% attendance in the class to appear in the Semester End Examination. Failing to obtain such a score will be given NOT QUALIFIED (NQ) and the student will not be eligible to appear in the End-Term examinations.

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 the period. If a student fails to attend a formal exam, quiz, test, etc. there won't be any provision for a re-exam.

8. Prescribed Books and References

Text Book

1. William Stallings, Cryptography and Network Security – Principles and Practice, 5th Edition, 2011, Prentice Hall.

Online References:

1. OWASP Top Ten, https://owasp.org/www-project-top-ten, OWASP Foundation
2. OWASP Code Review Guide Release 2.0, OWASP Foundation, Downloaded from https://owasp.org/www-project-code-review-guide/assets/OWASP_Code_Review_Guide_v2.pdf
3. OWASP Testing Guide 4.0, OWASP Foundation, Downloaded from https://owasp.org/www-project-web-security-testing-guide/assets/archive/OWASP_Testing_Guide_v4.pdf
4. Security and Privacy Controls for Information Systems and Organizations, NIST Special Publication 800-53 Revision 5 Downloaded from https://doi.org/10.6028/NIST.SP.800-53r5
5. Recent research papers and articles from various national and international journals and conferences

Reference Books

1. William Stallings, Network Security Essentials-Applications & Standards, Fourth Edition, 2011, Pearson.
2. Charlie Kaufman, Radia Perlman, Mike Speciner, Network Security Private Communication in a Public World, Second Edition, 2004, Pearson.
3. Eric Maiwald, Fundamentals of Network Security, 2004, Osborne/McGraw Hill, Dreamtech Press
4. Matt Bishop, Computer Security, Art and Science Addison-Wesley Professional, 2019