Course Title: **Network Security**

Course No. : ICT. Ed 575
Level: B.Ed
Semester: Seven

Nature of course: Theoretical + Practical
Credit Hour: 3 (2+1)
Teaching Hour: 80(32+48)

1. Course Description

The course, Network Security, is a major course for students studying towards acquiring the Bachelor of Education in Information Communication Technology (B. Ed. In ICT). This course is designed to provide fundamental skills needed to understand the internal and external security threats against a network, and to implement security policies that will protect an organization's information. The course objective is to impart fundamental understanding of every facet of information security, from the basics to advanced cryptography, authentication, secure web, email services and emerging best practices with security standards.

2. General Objectives

The general objectives of this course are as follows:

- Develop an understanding of information assurance as practiced in computer operating systems, distributed systems, networks and representative applications.
- Gain familiarity with prevalent network and distributed system attacks, defenses against them, and forensics to investigate the aftermath.
- Develop a basic understanding of cryptography, how it has evolved, and some key encryption techniques used today.
- Develop an understanding of security policies (such as authentication, integrity and confidentiality), as well as protocols to implement such policies in the form of message exchanges.

3. Course Outlines:

Specific Objectives	Contents	Hour
• Explain the concept of Computer Security. • Explain the OSI Security Architecture. • Classify the security attacks. • Explain the different security services. • Explain the mechanism for securing information in network. • Explain the Model of network security. • Discuss classical cryptography approaches.	**1. Introduction** 1.1 Computer Security Concept 1.2 The OSI Security Architecture 1.3 Security Attacks 1.4 Security Services 1.5 Security Mechanism 1.6 A Model for Network Security 1.7 Classical cryptography	10
• Differentiate between Cryptography and Cryptanalysis. • Explain the Feistel Cipher Structure. • Demonstrate the DES, 3DES, and AES algorithms.	**2. Symmetric Encryption and message Confidentiality** 2.1 Symmetric Encryption Principles 2.2 Symmetric Block Encryption Algorithms 2.3 Cipher Block Modes of Operations	12

• Explain the Cipher Block Modes: Electronic Codebook Mode, Cipher Block Chaining Mode, Cipher feedback Mode and Counter Mode		
• Explain the hash function requirements. • Demonstrate the SHA Secure hash function. • Demonstrate the working principle of MD. • Explain the Public-Key Encryption Structure. • Explain the Applications for Public-Key Cryptosystem. • Explain the requirements for Public-Key Cryptography. • Explain the RSA Public-Key Encryption Algorithm. • Explain the Diffie-Hellman Key Exchange algorithm. • Explain Digital signature algorithm with example.	**3. Public-Key Cryptography and Message Digest** 3.1 Secure Hash functions 3.2 Message Digest(MD) 3.3 Public-Key Cryptography Principles 3.4 Public-Key Cryptography Algorithms 3.5 Digital Signatures	16
• Explain the Public-Key Infrastructure Functions and Protocols. • Explain the different types of transport layer security. • Explain the different protocols of wireless security. • Explain the protocols used in email security. • Explain the mechanism of IP Security.	**4. Network Security Applications** 4.1 Public-Key Infrastructure 4.2 Transport Layer Security: SSL, HTTPs, Secure Shell(SSH) 4.3 Wireless Security: WEP, WAP, WPA2 4.4 E-Mail Security: PGP, S/MIME 4.5 IP Security	18
• Explain the different methods of intrusion detection. • Explain the different types of Malicious Software. • Explain the Characteristics and types of firewalls. • Implement the basic features of firewall.	**5. System Security** 5.1 Intruders 5.2 Malicious Software 5.3 Firewall	14
• Explain the basic concept of SNMP. • Explain the features of SNMPv1. • Explain the features of SNMPv3.	**6. Network management Security** 6.1 Basic Concept of SNMP 6.2 SNMPv1 6.3 SNMPv3	10

The practical aspect will focus on the uses and applications of information and network security software.

4. Laboratory:

- Analyze effects of different types of viruses and worms,
- Use encryption/decryption systems,

- Implementation of public/private key cryptography,
- Implementation of hash function,
- Issues of real time communication security
- Use and application of SSL
- Use network security tools

5. Instructional Techniques

The instructional techniques for this course are divided into two groups. First group consists of general instructional techniques applicable to most of the units. The second group consists of specific instructional techniques applicable to specific units.

5.1 General Techniques

- Providing the reading materials to the students to familiarize the units.
- Lecture, question-answer, discussion, brainstorming, practical, and buzz session.

5.2 Specific Instructional Techniques

Unit	Activity and instructional techniques	Teaching Hours(80)
1 to 6	Use network security tools to implement the algorithm	

6. Evaluation (Internal Assessment and External Assessment):

Nature of course	Internal Assessment	External Practical Exam/Viva	Semester Examination	Total Marks
Theory	40%	20%	40%	100%

***Note**: Students must pass separately in internal assessment, external practical exam / viva and or semester examination.*

6.1 Evaluation for Part I (Theory)

6.1.1 Internal Evaluation 40%

Internal evaluation will be conducted by course teacher based on following activities:

1) Attendance 5 points
2) Participation in learning activities 5 points
3) First assessment (written assignment) 10 points
4) Second assessment (Term examination) 10 points
5) Third assessment (Internal Practical Exam/Case Study) 10 points

Total 40 points

6.1.2 External Evaluation (Final Examination) 40%

Examination Division, office of the Dean, Faculty of Education will conduct final examination at the end of semester.

1) Objective type question (Multiple choice 10questionsx1mark) 10 marks
2) Short answer questions (6 questions x 5 marks) 30 marks

Total marks	40

6.2 **Evaluation for part II (practical) 20%**

Nature of the course	Semester final examination by External Examiner	Total percent
Practical	100%	100

6.2.1 Practical Examination Evaluation Scheme

a) External assessment ……100%
   i) Record book ……. 20%
   ii) Laboratory work exam/Case……..40%
   iii) VIVA……..40%

7. Recommended books and reading materials (including relevant published articles in national and international journals)

Stallings, William. *Network security essentials: applications and standards,* Delhi: Prentice Hall.

D. R. Stinson. *Cryptography: Theory and Practice*. CRC Press

Bishop, Matt. *Computer security: art and science*. Boston: Addison-Wesley.

Kaufman, C. (2002). *Network security: private communication in a public world* (2nd ed.). Delhi: Prentice Hall PTR.

Maiwald, E. (2004). *Fundamentals of network security*. Delhi: McGraw-Hill Technology Education.

Bictblogs.blogspot.com