

**Vikram University, Ujjain**

**Board of studies in Computer science (Faculty of Engineering Science)**

**SYLLABUS of  
Certificate Course in Network Security**

**Exclusively for University Teaching Department (ICS, VUU)**

**PROGRAMME of UTD (ICS, VUU)**

**(Effective from Academic Session 2020-21)**

**[Modified as according to the provision of “Ordinance ....”]**

**COURSE STRUCTURE**

**Certificate Course in Network Security**

<b>Paper code</b>	<b>Title of Paper</b>	<b>Theory External Marks</b>	<b>Min. Pass marks</b>	<b>Internal Marks</b>	<b>Min. Pass marks</b>	<b>Total</b>
<b>CNS -101</b>	<b>Data Communication and Computer Network</b>	<b>75</b>	<b>27</b>	<b>25</b>	<b>09</b>	<b>100</b>
<b>CNS- 102</b>	<b>Network Security</b>	<b>75</b>	<b>27</b>	<b>25</b>	<b>09</b>	<b>100</b>
<b>CNS -103</b>	<b>Internship/Industrial Training/Project Work</b>	<b><u>150</u></b>	<b><u>54</u></b>	<b>50</b>	<b>28</b>	<b>200</b>
	<b>Total</b>	<b><u>300</u></b>		<b>100</b>		<b>400</b>

## CNC-101 Data Communication and Computer Network

### UNIT-1

**Introduction:** Theoretical Model for Communication, analog and digital signals Bandwidth, Noise, Channel Capacity, Data-rate, Concepts of Circuit Switching, Message switching and Packet switching with their timing diagrams, comparison of switching techniques, ISDN.

### UNIT-2

**Evolution of Computer Networks Layered:** Network architecture, OSI Layers Model, transmission media topology, error detection & Correction techniques, Parity checks, CRC, Asynchronous and synchronous transmission, TDM, FDM.

### UNIT-3

**Data Link Layer:** Different Types of line discipline, simplex, half duplex and full duplex.**Flow control:** stop and wait protocol, sliding Window Protocol with their efficiency, ARQ techniques & their performances HDLC.

### UNIT-4

**LAN:** Static & Dynamic channel allocation, Media access control for LAN & WAN; **ALOHA:** pure, slotted ALOHA, CSMA, CSMA/CD, **IEEE 802 standards for LAN & MAN:** 802.3, 802.4, 802.5, 802.6 and 802.2 & their **comparison Fast LANs:** fast Ethernet, FDDI.

### UNIT- 5

**Routing:** Definition, Elements of routing techniques, Least Cost Routing algorithm, Dijkstra's algorithm, Bellman-ford algorithm, Routing Strategies, Congestion Control encryption & description techniques, Internet working, Internet and Intranet.

#### Reference Books:

1. Computer Networks Tanenbaum A. S. PHI.
2. LANs- Keizer
3. Computer Networks - Stalling w., PHI.

## **CNS -101: Network Security**

### **UNIT-1**

A Definition of Computer Security, The Challenges of Computer Security, The OSI Security Architecture. Security Attacks (Passive Attacks, Active Attacks). Security Services (Authentication, Access Control, Data Confidentiality, Data Integrity, Nonrepudiation, Availability Service).

### **UNIT-2**

Symmetric Encryption Principle (Cryptography, Cryptanalysis) Symmetric Block Encryption Algorithms (Data Encryption Standard, Triple DES, Advanced Encryption Standard). Stream Ciphers and RC4 (Stream Cipher Structure, The RC4 Algorithm). Cipher Block Modes of Operation (Electronic Codebook Mode, Cipher Block Chaining Mode, Cipher Feedback Mode, Counter Mode).

### **UNIT-3**

Public-Key Cryptography Principles (Public-Key Encryption Structure, Applications for Public-Key Cryptosystems, Requirements for Public-Key Cryptography). Public-Key Cryptography Algorithms (The RSA Public-Key Encryption Algorithm, Diffie-Hellman Key Exchange, Other Public-Key Cryptography Algorithms). Digital Signatures.

### **UNIT-4**

Approaches to Message Authentication: Secure Hash Functions (Hash Function Requirements, Security of Hash Functions, Simple Hash Functions, The SHA Secure Hash Function). Message Authentication Codes (HMAC, MACs Based on Block Ciphers).

### **UNIT-5**

**Security Threats and Vulnerability:** Types of attacks on Confidentiality, Integrity and Availability. Vulnerability and Threats, Malware: Viruses, Worms, Trojan horses, Security Counter Measures; Intrusion Detection Systems, Antivirus Software

#### **Reference Books:**

- W. Stallings, Cryptography and Network Security Principles and practice, 3/e, Pearson Education Asia, 2003. 2. Charlie Kaufman, Radia Perlman and Mike Speciner, “Network Security: Private Communication in a public world”, Prentice Hall India, 2nd Edition, 2002.
- Charles P. Pleege, “Security in Computing”, Pearson Education Asia, 5th Edition, 2001.
- William Stallings, “Network Security Essentials: Applications and standards”, Person Education Asia, 2000.
- W. Mao, Modern Cryptography: Theory & Practice, Pearson Education, 2004