Semester V

PROGRAMME: B. Sc (Information Technology)		Semester – V	
COURSE: NETWORK SECURITY		COURSE CODE: USIT501	
Periods per week 1 Period is 50 minutes	Lecture	5	
	Practical	3	
		Hours	Marks
Evaluation System	Theory Examination	2	60
	Theory Internal	--	40
	Practical		50

Unit I	**Computer Security :** Introduction, Need for security, Principles of Security, Types of Attacks **Cryptography :** Plain text and Cipher Text, Substitution techniques, Caesar Cipher, Mono-alphabetic Cipher, Polygram, Polyalphabetic Substitution, Playfair, Hill Cipher, Transposition techniques, Encryption and Decryption, Symmetric and Asymmetric Key Cryptography, Steganography, Key Range and Key Size, Possible Types of Attacks	**10 Lectures**
Unit II :	**Symmetric Key Algorithms and AES:** Algorithms types and modes, Overview of Symmetric key Cryptography, Data Encryption Standard (DES), International Data Encryption Algorithm (IDEA), RC4, RC5, Blowfish, Advanced Encryption Standard (AES)	**10 Lectures**
Unit III	**Asymmetric Key Algorithms, Digital Signatures and RSA:** Brief history of Asymmetric Key Cryptography, Overview of Asymmetric Key Cryptography, RSA algorithm, Symmetric and Asymmetric key cryptography together, Digital Signatures, Knapsack Algorithm, Some other algorithms (Elliptic curve cryptography, ElGamal, problems with the public key exchange)	**10 Lectures**
Unit IV	**Digital Certificates and Public Key Infrastructure (PKI):** Digital Certificates, Private Key Management, The PKIX Model, Public Key Cryptography Standards (PKCS), XML,PKI and Security, Hash functions, Key Predistribution, Blom's Scheme, Diffie-Hellman Key Predistribution, Kerberos, Diffie-Hellman Key Exchange, The Station-to-station Protocol	**10 Lectures**
Unit V	**Network Security, Firewalls and Virtual Private Networks:** Brief Introduction to TCP/IP, Firewalls, IP Security, Virtual Private Networks (VPN), Intrusion **Internet Security Protocols:** Basic concepts, Secure Socket Layer (SSL), Transport Layer Security (TLS), Secure Hyper Text Transfer Protocol (SHTTP), Time Stamping Protocol (TSP), Secure Electronic Transaction (SET), SSL vs SET, 3-D Secure Protocol, Electronic Money, E-mail Security, Wireless Application Protocol (WAP) Security, Security in GSM, Security in 3G	**10 Lectures**
Unit VI	**User Authentication and Kerberos:** Authentication basics, Passwords, Authentication Tokens, Certificate-based Authentication, Biometric Authentication, Kerberos, Key Distribution Center (KDC) , Security Handshake Pitfalls, Single Sign On (SSO) Approaches	**10 Lectures**

Books:

Cryptography and Network Security by Atul Kahate, 2nd Edition, Tata McGrawHill

(Unit I: Chapter 1,2, Unit II: Chapter 3, Unit III: Chapter 4, Unit IV: Chapter 5, Unit V: Chapter 6, Unit VI: Chapter 7)

References:

Cryptography and Network Security by William Stallings, Fifth Edition, Pearson Education.

Cryptography: Theory and Practice by *Douglas Stinson*, CRC Press, CRC Press LLC.