Course : ICT 103 : Information Security and Applications

Course Code	103
Course Title	Information Security and Applications
Credit	4
Teaching per Week	4 Hrs
Minimum weeks per Semester	15 (Including Class work, examination, preparation, holidays etc.)
Last Review / Revision	June 2019
Purpose of Course	This course is designed to provide students with the necessary background and knowledge to identify security risks and develop appropriate counter measures.
Course Objective	To provide an understanding of principal components, major issues, technologies, and basic approaches in information security
Pre-requisite	Basic concepts of computer network
Course Out come	This would help students to understand vulnerability of applications and encourage them to embed security in various applications they develop.
Course Content	**Unit 1 : Introduction to Information Security** 1.1 Introduction to Security 1.2 Need for Security 1.3 The OSI Security Architecture 1.4 Security Attacks 1.4.1 Active attacks 1.4.2 Passive Attacks 1.5 Security Services 1.6 Security Mechanism **Unit 2 : Cryptography** 2.1 Classical Encryption Techniques 2.1.1 The substitution and Transposition Techniques 2.1.3 The Hill Cipher, Vignere Cipher 2.1.4 Rotor Machines 2.1.5 Steganography 2.1.6 Theoretical Security and Computational Security 2.1.7 Motivation for Product Cryptosystems 2.2 Symmetric key cryptography 2.2.1 Block Cipher Principles 2.2.2 Data Encryption Standard (DES) 2.2.3 Advanced Encryption Standard (AES) 2.2.4 Attacks on DES and AES 2.2.5 Block Cipher modes of Operation 2.2.6 Introduction to Stream Cipher 2.2.6.1 RC4 Algorithm 2.3 Asymmetric Key cryptography 2.3.1 Principles of Public Key Cryptosystem 2.3.2 The RSA Algorithm 2.3.3 Attacks on RSA 2.3.4 Key Management 2.3.4.1 Key Distribution Scenarios 2.3.4.2 Key Management 2.3.4.3 Diffie Hellman Key Exchange **Unit 3 : Integrity , Authentication and Hash Functions** 3.1 Introduction 3.2 Authentication Requirements & its functions 3.3 Message Authentication 3.3.1 Message Authentication Codes 3.3.2 Hash Functions 3.3.3 MD5, SHA algorithms

	3.3.4 Applications of SHA (e.g BlockChain) 3.4 User Authentication 3.4.1 Remote User Authentication Principles 3.4.2 Remote User Authentication using Symmetric Encryption 3.4.3 Kerberos 3.5 Digital Signatures and Authentication Protocols 3.5.1 Introduction to digital signatures 3.5.2 Authentication Protocols 3.5.3 Digital Signature Standard **Unit 4 : Network /IP Security** 4.1 IP Security Overview 4.2 Security in IPV4 and IPV6, Tradeoff involved 4.3 Encapsulating Security Payload 4.4 Security Associations 4.5 Internet Key Exchange 4.6 Cryptographic Suites 4.7 Firewalls 4.8 Biometrics **Unit 5 : Transport and Application Layer Security** 5.1 Web Security Issues 5.2 Secure Socket Layer(SSL) 5.3 Transport Layer Security 5.4 HTTPS 5.5 Secure Shell 5.6 Email Security: PGP,SMIME
Reference Book	1. Cryptography and Network Security – Principles and Practice – William Stallings- Seventh Edition- Pearson Publication 2. Cryptography and Network Security- Behrouz A. Forouzan – McGrawHill Publication 3. Information Security: Theory and Practice – Dhiren R. Patel – PHI
Teaching Methodology	Class Room Teaching, Discussion and Assignment
Evaluation Method	30% Internal assessment 70% External assessment