CSI3002	Applied Cryptography and Network Security	L	T	P	J	C
		2	0	2	0	3
Pre-requisite	**Nil**	**Syllabus version**				
		1.0				

Course Objectives:

1. To learn the emerging concepts of cryptography and algorithms
2. To defend the security attacks on information systems using secure algorithms and Authentication process
3. To categorize and analyze the key concepts in network and wireless security

Course Outcome:

1. Infer the need of security to introduced strong cryptosystems.
2. Analyze the cryptographic algorithms for information security.
3. Identify the authentication schemes for membership authorization.
4. Identify computer and network security threats, classify the threats and develop a security model for detect and mitigate the attacks.
5. Identify the requirements for secure communication and challenges related to the secure web services
6. Identify the need of ethical and professional practices, risk management using emerging security solutions.

Student Learning Outcomes (SLO):	**1, 9, 18**	
Module:1	**Introduction to Cryptography**	**4 hours**
Security trends, Security attacks, Security mechanism, Elementary number theory, Pseudo-random bit generation. **Basic security services:** confidentiality, integrity, availability, non-repudiation, privacy.		
Module:2	**Symmetric Key Cryptography**	**4 hours**
Block Ciphers: DES, Triple-DES, AES, Modes of Operation, Stream Cipher		
Module:3	**Asymmetric Key Cryptography**	**4 hours**
RSA, Elgamal, Elliptic Curve Cryptography (ECC), Diffie-Hellman key exchange protocol		
Module:4	Hash Functions and Authentication	**4 hours**
Message Authentication Code (MAC), MD5, Secure Hash algorithms (SHA), HMAC, Digital Signatures, Digital Signature Standard (DSS).		
Module:5	**Basic Applied Cryptography**	**3 hours**
Key management and distribution, digital certificates, identity-based encryption, Identification and authentication, zero knowledge protocols		
Module:6	**Advanced Applied cryptography**	**5 hours**
Side-channel attack, Pretty Good Privacy (PGP), S/MIME, Kerberos, Homomorphic encryption, Quantum Cryptography, DNA Cryptography, Chaos Based Cryptosystem		
Module:7	**Web and Wireless Security**	**4 hours**
IPsec: AH and ESP, IKE- SSL/TLS, Types of Firewalls, Intrusion detection and Prevention systems, Wireless Application Protocol (WAP)		
Module:8	Recent Trends	**2 hours**
	Total Hours:	**30 hours**

List of Experiments

1	Implement DES, Triple DES and AES Key Algorithms	**4 Hours**
2	Implement RSA, ECC and Diffie-Hellman Key Establishment.	**4 Hours**
3	Implement a Secret-Sharing algorithm and Homomorphic Encryption algorithm	**2 Hours**
4	Implement message authentication (MAC) and HASH algorithms	**3 Hours**
5	Consider and examine the Wireless network security and technology	**2 Hours**

	integration for compliance using the case study of Cisco.	
6	Explore the Snort Intrusion Detection Systems. Study Snort IDS, a signature-based intrusion detection system used to detect network attacks. Snort can also be used as a simple packet logger. For the purpose of this lab the students will use snort as a packet sniffer and write their own IDS rules	**4 Hours**
7	Explore ways to perform wireless attacks and understand potential defences. The attacks that will be covered are inspecting & modifying wireless card parameters, changing the wireless transmission channel, flooding attacks, and cracking keys of WPA2 protected networks.	**4 Hours**
8	Pretty Good Privacy – • Create a public/private key pair in PGP • Create a revocation ley • Exchange PGP keys with other students • Signing the new key • Encrypting a file using your partner's public key • Decrypting the file using your private key • Encrypting and signing a file • Verifying the signature • Sending secure Email with PGP • Adding a public key and sending secure email.	**4 Hours**
9	Send and receive an encrypted email message using S/MIME.	**3 Hours**
	Total Lecture hours:	**30 hours**

Text Book(s)	
1.	W. Stallings, Cryptography and Network Security: Principles and Practice, 7th Ed. Pearson Publishers, 2017.
2.	Behrouz A. Forouzan, Cryptography and Network Security:6th Ed. McGraw-Hill, 2017.

Reference Books	
1.	Kaufman, Perlman and Speciner. Network Security: Private Communication in a Public World., 2nd edition, Pearson Publishers, 2002.
2	Menezes, van Oorschot, and Vanstone, The Handbook of Applied Cryptography, 20th Edition, WILEY, 2015
3	H. Silverman, A Friendly Introduction to Number Theory, 4th Ed. Boston: Pearson, 2012.

Mode of Evaluation: CAT / Assignment / Quiz / FAT / Lab			
Recommended by Board of Studies	11-02-2021		
Approved by Academic Council	No. 61	Date	18.02.2021