CSEN2071	CRYPTOGRAPHY AND NETWORK SECURITY	L	T	P	S	J	C
		3	0	0	0	0	3
Pre-requisite							
Co-requisite							
Preferable exposure	None						

Course Description:

The aim of this course is to introduce information security concepts to the students. This course develops a basic understanding of goals, threats, attacks and mechanisms, algorithms, and their design choices. The course also familiarizes students with a few mathematical concepts used in cryptology. The course emphasizes to give a basic understanding of attacks in cryptosystems and how to shield information from attacks. It also deals with message authentication, Digital signatures, and Network security.

Course Educational Objectives:

- Understand basics of security concepts and comprehend Classical Encryption Techniques
- Impart various symmetric cryptographic techniques
- Learn number theory related to RSA and Diffie-Hellman algorithms
- Study different hash functions and message authentication techniques
- Impart knowledge of application and transport layers security concepts

UNIT 1 Basics of Computer Networks 9 hours

Introduction: Computer Security Concepts, The OSI Security Architecture, Cryptography,

cryptanalysis, attacks, services, security mechanisms.

Classical Encryption Techniques: Substitution Techniques, Caesar Cipher, Monoalphabetic Ciphers, Play fair Cipher, Hill Cipher Polyalphabetic Ciphers. Transposition Techniques.

UNIT 2 Symmetric key Cryptography 9 hours

Symmetric Key Cryptography: Block Ciphers and the Data Encryption Standard (DES) algorithm. Differential and linear cryptanalysis, triple DES. Block cipher design principles, Block cipher modes of operation, Advanced Encryption Standard (AES), Stream Ciphers: RC4.

UNIT 3 Number theory & Cryptography 9 hours

Number theory: Divisibility and The Division Algorithm, The Euclidean Algorithm, Modular Arithmetic, Prime Numbers, Fermat's and Euler's Theorems, Testing for Primality, The Chinese Remainder Theorem. Public Key

Cryptography: Principles of public key cryptosystem, RSA algorithm, security of RSA. Diffie Hellman key exchange.

UNIT 4 Cryptographic Hash Functions 9 hours

Cryptographic Hash Functions: Applications of hash Functions, Secure Hash Algorithm (SHA). MAC and Digital Signatures: Message Authentication Requirements, Message Authentication Functions, Requirements for Message Authentication Codes, HMAC, DAA and CMAC. Digital signatures, Digital Signature Standard (DSS), Key management and distribution: Distribution of Public Keys, X.509 Certificates.

UNIT 5 Internet Security 9 hours

Internet Security: Introduction to SSL and TLS. Email Security: S/MIME. Firewalls: Types of Firewalls, configuring firewalls, Intrusion Detection and Preventions Systems.

Textbooks:

1. William Stallings, Cryptography and Network Security – Principles and Practice, 7/e. Pearson Education, 2017.

References:

1. Behrouz A Fourozen and Debdeep Mukhopadhyay, Cryptography and Network Security,3/e,McGraw Hill, 2015
2. Atul Kahate, Cryptography and Network Security, 4/e, McGraw Hill, 2019.
3. Buchmann, Introduction to Cryptography, Springer, 2004
4. Bruce Schneier, Applied Cryptography: Protocols, Algorithms, and Source Code in C(cloth),2/e, Publisher: John Wiley& Sons, Inc., 1996.
5. Chwan-Hwa(John) Wu, Introduction to Computer Networks and Cybersecurity, CRC Press,2013
6. https://www.coursera.org/learn/introduction-cybersecurity-cyber-attacks/home/week/3
7. https://www.coursera.org/learn/cybersecurity-roles-processes-operating-system-security/home/week/1
8. https://www.coursera.org/learn/cybersecurity-compliance-framework-system-administration/home/week/1

Course Outcomes:

After successful completion of the course the student will be able to:
1. illustrate working of classical encryption techniques
2. describe the working of symmetric encryption techniques
3. experiment the working of public key cryptography algorithms such as RSA, Diffie-Hellman
4. Apply Hash functions and message authentication techniques
5. Demonstration of firewall configuration.

CO-PO Mapping:

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3
CO1	2	2	1												
CO2	1	2	2	1											
CO3	2	2	2	1											
CO4	2	1	2	1		1		1							
CO5	2	1	2	1		1		1							

Note: 1 - Low Correlation 2 - Medium Correlation 3 - High Correlation

APPROVED IN:

BOS : 06-09-2021 **ACADEMIC COUNCIL: 01-04-2022**

SDG No. & Statement:

SDG 16: Provides safety and security to the citizens of the county in cyberspace, which creates peaceful and inclusive societies

SDG Justification: