Course Code	Course Title	Credits	Lectures /Week
USCS502	**Information & Network Security**	**2**	**3**

About the Course: This course provides an in-depth understanding of the principles and techniques used in computer and network security. Students will explore various security topics, including encryption techniques, public-key cryptography, key management, message authentication, digital signatures, authentication protocols, network security, web security, intrusion detection, malicious software, and firewall design principles. Through theoretical learning and practical exercises, students will develop the necessary knowledge and skills to analyze, design, and implement secure systems and protect against security threats.

Course Objectives:

- Familiarize students with the fundamental principles, models, and mechanisms of computer and network security.
- Explore various encryption techniques, including symmetric and public-key cryptography, and understand their strengths, weaknesses, and real-world applications.
- Examine different authentication and key management methods to ensure secure communication and protect against unauthorized access.
- Understand the concepts and techniques of message authentication, digital signatures, and authentication protocols used in secure communication systems.
- Investigate network security measures, including IP security, web security, intrusion detection, malicious software detection, and firewall design principles.

Learning Outcomes:

After successful completion of this course, students would be able to:

- Analyze and evaluate security trends, attacks, and mechanisms, and propose effective security solutions based on the OSI security architecture.
- Apply classical encryption techniques, such as substitution and transposition ciphers, to encrypt and decrypt messages and analyze their security implications.
- Implement public-key cryptography algorithms, including RSA, and demonstrate the ability to securely exchange keys and establish secure communication channels.
- Design and implement secure authentication mechanisms, including message authentication codes and digital signatures, to ensure data integrity and non-repudiation.
- Evaluate and implement various security measures, such as IP security, web security protocols (e.g., SSL/TLS), intrusion detection systems, and firewall configurations, to protect networks and systems from unauthorized access and attacks.

Unit	Topics	No of Lectures
I	**Introduction:** Security Trends, The OSI Security Architecture, Security Attacks, Security Services, Security Mechanisms **Classical Encryption Techniques:** Symmetric Cipher Model, Substitution Techniques, Transposition Techniques, Steganography, Block Cipher Principles, The Data Encryption Standard, The Strength of DES, AES (round	15

	details not expected), Multiple Encryption and Triple DES, Block Cipher Modes of Operation, Stream Ciphers **Public-Key Cryptography and RSA:** Principles of Public-Key Cryptosystems, The RSA Algorithm	
II	**Key Management:** Public-Key Cryptosystems, Key Management, Diffie-Hellman Key Exchange **Message Authentication and Hash Functions:** Authentication Requirements, Authentication Functions, Message Authentication Codes, Hash Functions, Security of Hash Functions and Macs, Secure Hash Algorithm, HMAC **Digital Signatures and Authentication:** Digital Signatures, Authentication Protocols, Digital Signature Standard **Authentication Applications:** Kerberos, X.509 Authentication, Public-Key Infrastructure	**15**
III	**Electronic Mail Security:** Pretty Good Privacy, S/MIME **IP Security:** Overview, Architecture, Authentication Header, Encapsulating Security Payload, Combining Security Associations, Key Management **Web Security:** Web Security Considerations, Secure Socket Layer and Transport Layer Security, Secure Electronic Transaction **Intrusion:** Intruders, Intrusion Techniques, Intrusion Detection **Malicious Software:** Viruses and Related Threats, Virus Countermeasures, DDOS **Firewalls:** Firewall Design Principles, Types of Firewalls	**15**

Textbook(s):

1. Cryptography and Network Security: Principles and Practice 7th edition, William Stallings, Pearson

Additional Reference(s):

1. Cryptography and Network, 2nd edition, Behrouz A Fourouzan, Debdeep Mukhopadhyay, TMH.
2. Atul Kahate, “Cryptography and Network Security”, Tata McGraw-Hill.