Subject Code **20CST354**	**Introduction to Information Security and Cryptography**	**L**	**T**	**P**	**C**
	Total Contact Hours: 45Hours	**3**	**0**	**0**	**3**
	Common to all Specializations of CSE is 4thYear				
	Prerequisite: Studied Computer Networks, Operating System, Design and Analysis of Algorithms				

Course Objectives

1. To familiarize the students with the basic concepts of services, attacks with its models and concepts of encryption.
2. To conceptualize digital signature and different encryption algorithm. To state

   the various authentication protocols and their requirements.
3. To elucidate an application of security and their effects on security standards.
4. To comprehend IP security and their methods.
5. To familiarize the student this basic encryption and decryptions

Course Outcomes

CO1	Analyze the number theory,classical encryption techniques and block ciphers.
CO2	Understand and analyze public-key cryptography, encryption standards, RSA, and other public-key cryptosystems.
CO3	Design hash functions, MAC algorithms and digital signatures.
CO4	Explore best security practice and system security such as authentication schemes, firewall characteristics and configurations.
CO5	Demonstrate and examine the various encryption techniques to secure data in transit across network.

UNIT-I

Introduction & Number Theory: Services, Mechanisms and attacks-the OSI security architecture-Network security model-Classical Encryption techniques (Symmetric cipher model, substitution techniques, transposition techniques, steganography). Finitefields and Number Theory: Groups, Rings, Fields-Modular arithmetic-Euclid‟s algorithm-Finite fields- Polynomial Arithmetic –Prime numbers- Fermat‟s and Euler‟s theorem-Testing for primality -The Chinese remainder theorem- Discrete algorithms.

Block Ciphers: Data Encryption Standard-Block cipher principles-block cipher modes of operation-Advanced Encryption Standard (AES)-Triple DES-Blowfish-RC5 algorithm.

UNIT II

Public key cryptography: Principles of public key cryptosystems-The RSA algorithm-Key management – Diffie Hellman Key exchange

Hash Functions and Digital Signatures: Authentication requirement – Authentication function – MAC – Hash function – Security of hash function and MAC – MD5–SHA512–HMAC – CMAC – Digital signature and authentication protocols – DSS – EI Gamal – Schnorr.

UNIT III

Security Practice & System Security: Authentication applications – Kerberos – Authentication services – Internet Firewalls for Trusted System: Roles of Firewalls – Firewall related terminology- Types of Firewalls – Firewall designs –Intruder – Intrusion detection system – Virus and related threats.

E-mail Security: Security Services for E-mail-attacks possible through E-mail – establishing keys privacy-authentication of the source-Message Integrity-Privacy-S/MIME.

IPSecurity and Web Security: Overview of IP Security – IP Address and IPv6-Authentication Header-Encapsulation Security Payload (ESP)- SSL Architecture and its layers- Transport Layer Security (TLS)-HTTPS- Secure Shell (SSH)

Text Books:

1. William Stallings, Cryptography and Network Security, 6th Edition, Pearson Education, March 2013.
2. Charlie Kaufman, Radia Perlman and Mike Speciner, "Network Security", Prentice Hall of India, 2002.

Reference Books:

1. Behrouz A. Ferouzan, "Cryptography & Network Security", Tata MC GrawHill.
2. Man Young Rhee, "Internet Security: Cryptographic Principles", "Algorithms and Protocols", WileyPublications.
3. Charles Pfleeger, "Security in Computing", 4th Edition, Prentice Hall ofIndia.
4. Ulysess Black, "Internet Security Protocols", Pearson EducationAsia.
5. Charlie Kaufman and Radia Perlman, Mike Speciner, "Network Security, Second Edition, Private Communication in Public World",PHI.
6. William Stallings, "Network Security Essentials (Applications and Standards)", 4th Edition, Pearson Education. ,2012

Mode of Evaluation: The performance of students is evaluated as follows:

	Theory	
Components	**Continuous Internal Assessment (CAE)**	**Semester End Examination (SEE)**
Marks	**40**	**60**
Total Marks	**100**	

Relationship between the Course Outcomes (COs) and Program Outcomes (POs)

Mapping Between COs and POs		
SN	**Course Outcome (CO)**	**Mapped Program Outcome (PO)**
1	Analyze the number theory. classical encryption techniques and block ciphers.	Discuss the basics of number theory, network security and cryptography algorithms.
2	Understand and analyze public-key cryptography, encryption standards, RSA, and other public-key cryptosystems.	Explain the various standards Symmetric Encryption algorithms used to provide confidentiality.
3	Design hash functions, MAC algorithms and digital signatures.	Explain the various standards Asymmetric Encryption algorithms to achieve authentication.
4	Explore best security practice and system security such as authentication schemes, firewall characteristics and configurations.	Explore the knowledge of key exchange protocols.Examine the effects on digitized security.
5	Demonstrate and examine the various encryption techniques to secure data in transit across network.	Demonstrate encryption techniques to secure data in transit across network.

Mapping Between COs and POs														
COs	**PO1**	**PO2**	**PO3**	**PO4**	**PO5**	**PO6**	**PO7**	**PO8**	**PO9**	**PO10**	**PO11**	**PO12**	**PSO1**	**PSO2**
CO1	1	–	–	2	–	–	–	–	–	–	–	–	–	–
CO2	1	3	2	1	–	–	–	–	–	–	–	–	–	2
CO3	1	3	2	1	–	–	–	–	–	–	–	–	–	2
CO4	2	2	1	1	–	–	–	–	–	–	–	–	–	2
CO5	2	2	2	1	–	–	–	–	–	–	–	–	–	3

		Engineering Knowledge	Problem analysis	Design/development of solutions	Conduct investigations of complex	Modern tool usage	The engineer and society	Environment and sustainability	Ethics	Individual or team work	Communication	Project management and finance	Life-long Learning
Course Code	Course Name	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**
20CST354	**Introduction to Information Security**												

1 = addressed to small extent
2 = addressed significantly
3 = major part of course