CS-703: INFORMATION SECURITY

Teaching and Examination Scheme:

Teaching Scheme			Credits	Marks			Duration of End Semester Examination
L	T	P/D	C	Sessional	End Semester Exams	Total	
3	1	0	4	40	60	100	3Hrs

COURSE OBJECTIVE:

The course should enable the students to know the methods of conventional encryption, public key encryption, number theory. Understanding hash functions and various network security tools.

COURSE CONTENT:

UNIT	CONTENT	No. of Hrs.
I	**Importance of information system:** Basic of information system, security goals, techniques for security goal implementation. **Mathematical Background for Cryptography**: Modular arithmetic, greatest common divisor, Euclidean algorithm, computing the inverse, extended Euclidean algorithm, Fermat's theorem, Euler totient function. Role of cryptography in information security, plain text, cipher text, key, encryption, decryption, Kerckhoff's principle. substitution ciphers, transposition ciphers, types of attacks on ciphers	10
II	**Introduction to Ciphers:** Monoalphabetic and polyalphabetic ciphers, perfect substitution cipher such as the vernam cipher, stream and block cipher, confusion and diffusion, unicity distance. **Cryptanalysis:** Introduction of cryptanalysis, cryptanalysis of monoalphabetic ciphers such as affine cipher, cryptanalysis of polyalphabetic ciphers such as vigenere cipher	10
III	**Public key(Asymmetric key) Encryption Systems**: Concept and characteristics of public key encryption system, introduction to Merkle-Hellman knapsacks, Rivest–Shamir-Adlman (RSA) encryption. **Digital Signature**: Introduction to digital signature algorithms, RSA digital signature scheme algorithm, the digital signature standard (DSA).	10
IV	**Secure Secret Key (Symmetric) Systems:** The data encryption standard (DES), introduction to advance encryption standard (AES). **Law and legal Framework**: Information security and law, understanding the law for information security, the Indian IT act, patent law, copyright law, Indian copyright law, privacy on internet, privacy consideration in web services, ethical issue owing to information warfare, cryptographic tools and ethical issues, understanding ethical hacking,	9

97

Dean
H.P. Technical University
Hamirpur - 177001

	social engineering issue, ethical domain for information security.	

Text Books:

1. Behrouz A Farouzan , ***"Cryptography and N/W Security"***, McGraw Hill.
2. Charles P.Pfleeger, ***"Security in Computing"***, Prentice Hall International, Inc.

Reference Books:

1. Nina Godbole, ***"Information System security"***, Wiley India Publication
2. Eric Cole & Ronald Krutz, ***"Network Security bible"*** , Wiley India Publication.
3. Patel , ***"Information security"***, PHI publication.
4. C K Shyamala & N Harini, ***"Cryptography and Security"*** , Wiley India publication
5. William Stallings, ***"Cryptography and N/W Security"***, Pearson.