ITE5003 Cryptography and Network Security

	LTP J C **3 0 0 4 4**
Pre-Req: NIL	

Objectives:

1. To understand the cryptographic techniques like encryption, key exchange and digital signature techniques used today.
2. To learn the security policies such as authentication, integrity and confidentiality.
3. To understand the security issues in web and network scenario.

Expected Outcome :

On completion of this course, student should be able to

1. Implement the security policies such as authentication, integrity and confidentiality in the form of message exchanges.
2. Implement cryptographic techniques used today and analyze its vulnerabilities against various threats.
3. Analyze web and network security threats.

Module	Topics	L Hrs	SLO
1	**Introduction:** Symmetric cipher model, substitution and transposition ciphers, DES, strength of DES, Triple DES, Block cipher design principles.	5	1,2
2	**Symmetric ciphers:** AES structure, transformation function and key expansion, RC4, RC6, Idea, Blowfish	5	1,2
3	**Number Theory concepts:** Prime numbers, prime factorization, Euclidean algorithm, Fermat's and Euler's theorem, modular arithmetic, Chinese remainder theorem.	5	1
4	**Asymmetric ciphers:** Principles of public-key cryptosystem, RSA algorithm, attacks over RSA algorithm, Elgamal crypto system, Elliptic curve cryptography, pseudorandom number generation.	7	1,2
5	**Key management and data integrity:** Symmetric key sharing using symmetric and asymmetric approach, Distribution of public keys, X.509certificates, public key infrastructure, Two simple hash functions, HMAC, SHA-3, RSA-PSS digital signature algorithm.	5	1,2
6	**Network and Cloud Security:** Network access control, Extensible authentication protocol, IEEE 802.1 port-based network access control, Cloud security risks and countermeasures, Data protection in the cloud, Cloud security as a service, IP Security.	8	2
7	**Internet Security:** Transport level security-SSL, HTTPS, Secure Shell, Mobile device security, IEEE 802.11i Wireless LAN Security, E-Mail Security, E-Business security.	7	2
8	**Expert talk on recent trends**	3	17

<table>
<tr><td><b>Total Lecture Hours</b>
<b># Mode:</b> Flipped Class Room, [Lecture to be videotaped], Use of physical and computer models to lecture, Visit to Industry, Min of 2 lectures by experts</td><td><b>45</b></td></tr>
<tr><td colspan="2">TextBooks
1. William Stallings, “Cryptography and Network Security: Principles and Practices”, 6th Edition, Pearson education, 2014.

Reference Books
1. Charles P.Pfleeger, Shari Lawrence P.Pfleeger, Jonathan Margulies, “Security in Computing”, 5th Edition, Prentice Hall, 2015.
2. Atul Kahate, “Cryptography and Network Security”, 3rd Edition, Tata McGraw Hill, 2013.</td></tr>
<tr><td colspan="2">Compiled by : Prof. P.M. Durai Raj Vincent</td></tr>
</table>