Course Code:	Course Title	Credit
CSC602	Cryptography & System Security	3

Prerequisite: Computer Networks	
Course Objectives:	
1	To introduce classical encryption techniques and concepts of modular arithmetic and number theory.
2	To explore the working principles and utilities of various cryptographic algorithms including secret key cryptography, hashes and message digests, and public key algorithms
3	To explore the design issues and working principles of various authentication protocols, PKI standards and various secure communication standards including Kerberos, IPsec, and SSL/TLS.
4	To develop the ability to use existing cryptographic utilities to build programs for secure communication
Course Outcomes:	
1	Understand system security goals and concepts, classical encryption techniques and acquire fundamental knowledge on the concepts of modular arithmetic and number theory
2	Understand, compare and apply different encryption and decryption techniques to solve problems related to confidentiality and authentication
3	Apply different message digest and digital signature algorithms to verify integrity and achieve authentication and design secure applications
4	Understand network security basics, analyse different attacks on networks and evaluate the performance of firewalls and security protocols like SSL, IPSec, and PGP
5	Analyse and apply system security concept to recognize malicious code

Module		Content	Hrs
1		**Introduction - Number Theory and Basic Cryptography**	**8**
	1.1	Security Goals, Attacks, Services and Mechanisms, Techniques. Modular Arithmetic: Euclidean Algorithm, Fermat‘s and Euler‘s theorem	
	1.2	Classical Encryption techniques, Symmetric cipher model, mono-alphabetic and polyalphabetic substitution techniques: Vigenere cipher, playfair cipher, Hill cipher, transposition techniques: keyed and keyless transposition ciphers	
2		**Symmetric and Asymmetric key Cryptography and key Management**	**11**
	2.1	Block cipher principles, block cipher modes of operation, DES, Double DES, Triple DES, Advanced Encryption Standard (AES), Stream Ciphers: RC4 algorithm.	
	2.2	Public key cryptography: Principles of public key cryptosystems- The RSA Cryptosystem, The knapsack cryptosystem	
	2.3	Symmetric Key Distribution: KDC, Needham-schroeder protocol. Kerberos: Kerberos Authentication protocol, Symmetric key agreement: Diffie Hellman, Public key Distribution: Digital Certificate: X.509, PKI	
3		**Cryptographic Hash Functions**	**3**
	3.1	Cryptographic hash functions, Properties of secure hash function, MD5, SHA-1, MAC, HMAC, CMAC.	
4		**Authentication Protocols & Digital Signature Schemes**	**5**
	4.1	User Authentication, Entity Authentication: Password Base, Challenge Response Based	

	4.2	Digital Signature, Attacks on Digital Signature, Digital Signature Scheme: RSA	
5		**Network Security and Applications**	**9**
	5.1	Network security basics: TCP/IP vulnerabilities (Layer wise), Network Attacks: Packet Sniffing, ARP spoofing, port scanning, IP spoofing	
	5.2	Denial of Service: DOS attacks, ICMP flood, SYN flood, UDP flood, Distributed Denial of Service	
	5.3	Internet Security Protocols: PGP, SSL, IPSEC. Network security: IDS, Firewalls	
6		**System Security**	**3**
	6.1	Buffer Overflow, malicious Programs: Worms and Viruses, SQL injection	

Textbooks:	
1	William Stallings, ***"Cryptography and Network Security, Principles and Practice"***, 6th Edition, Pearson Education, March 2013
2	Behrouz A. Ferouzan, ***"Cryptography & Network Security"***, Tata McGraw Hill
3	Behrouz A. Forouzan & Debdeep Mukhopadhyay, ***"Cryptography and Network Security"*** 3rd Edition, McGraw Hill

Referecebooks:	
1	Bruce Schneier, ***"Applied Cryptography, Protocols Algorithms and Source Code in C",*** Second Edition, Wiley.
2	Atul Kahate, ***"Cryptography and Network Security",*** Tata McGraw-Hill Education, 2003.
3	Eric Cole, ***"Network Security Bible",*** Second Edition, Wiley, 2011.

Assessment:	
Internal Assessment:	
Assessment consists of two class tests of 20 marks each. The first class test is to be conducted when approx. 40% syllabus is completed and second class test when additional 40% syllabus is completed. Duration of each test shall be one hour.	
End Semester Theory Examination:	
1	Question paper will comprise of total six questions.
2	All question carries equal marks
3	Questions will be mixed in nature (for example supposed Q.2 has part (a) from module 3 then part (b) will be from any module other than module 3)
4	Only Four question need to be solved.
5	In question paper weightage of each module will be proportional to number of respective lecture hours as mention in the syllabus.

Useful Links	
1	https://github.com/cmin764/cmiN/blob/master/FII/L3/SI/book/W.Stallings%20-%20Cryptography%20and%20Network%20Security%206th%20ed.pdf
2	https://docs.google.com/file/d/0B5F6yMKYDUbrYXE4X1ZCUHpLNnc/view