CENTRAL UNIVERSITY OF KERALA
DEPARTMENT OF COMPUTER SCIENCE
M.Sc. COMPUTER SCIENCE

CORE COURSE					
COURSE CODE	COURSE TITLE	CONTACT HRS/WEEK			CREDITS
		LEC	LAB	TUT	
CSC5201	Cryptography and Network Security	2	2	1	4

Lec = Lecture, Tut = Tutorial, Lab = Practical

This is a participatory, experimental and problem solving **skill development course**.

Course Objective

The objective of the course is to provide theoretical and practical aspects of cryptography and network security.

By completing this course, students will obtain the following course/learning outcomes:

1. Knowledge gained:
   - (i) Evaluate security mechanisms using rigorous approaches by key ciphers and Hash functions
   - (ii) Identify and classify particular examples of attacks and factors driving the need for network security
   - (iii) Compare and contrast symmetric and asymmetric encryption systems
   - (iv) Usage of network security tools and applications to understand the system level security
2. Skill gained:
   - (v) Critically Analyse the vulnerabilities in any computing system
3. Competency gained:
   - (vi) Conduct research in cryptography and network security

Prerequisites: Basic knowledge in number theory.

Grading:

Lab experiments and implementation	– 15%
Participatory based group Project	– 10%
Class Test/Assignment/Quiz/presentation	– 5%
Lab Test	- 10%
Final Exam	– 60%

CSC5201 - Cryptography and Network Security

Module 1

Introduction to security attacks, services and mechanism, Classical encryption techniques substitution ciphers and transposition ciphers, Stream and block ciphers, cryptanalysis, steganography. Modern Block Ciphers: Block ciphers principles, Shannon's theory of confusion and diffusion, fiestal structure, Data encryption standard (DES), Strength of DES, Triple DES.

Module 2

Advanced Encryption Standard (AES) encryption and decryption, Principals of public key crypto systems, RSA algorithm, Other Public-Key Cryptosystems. Hash functions, security of hash functions, Secure hash algorithm (SHA), Message Authentication Codes, Digital Signatures, Digital signature standards (DSS).

Module 3

Key Management and distribution: Symmetric key distribution, Diffie-Hellman Key Exchange, Public key distribution, X.509 Certificates, Public key Infrastructure. Authentication Applications: Kerberos Electronic mail security: pretty good privacy (PGP), S/MIME.

Module 4

IP Security: Architecture, Authentication header, encapsulating security payloads, combining security associations, key management. System Security: Intruders, Intrusion detection, Malicious software, firewalls.

Module 5

Case Studies on Cryptography and Security: Cryptographics solution, Denial of Service Attacks, IP Spoofing Attacks, Cross Site Scripting Vulnerability, Contract Signing, Secret Splitting, Creating a VPN

Text books:

1. William Stallings, *Cryptography and Network Security*, Pearson Education, 5th Edition, 2011
2. Forouzan Mukhopadhyay, *Cryptography and Network Security*, Mc Graw Hill, 2nd Edition, 2010
3. Michael E. Whitman, Herbert J. Mattord, *Principles of Information Security*, Cengage Learning, 4th Edition, 2012

Reference:

4. R. Rajaram, *Network Security and Cryptography*, SciTech Publication, First Edition, 2013.
5. C. K. Shyamala, N. Harini, T. R. Padmanabhan, *Cryptography and Network Security*, Wiley India, 1st Edition, 2011.
6. Bernard Menezes, *Network Security and Cryptography*, CENGAGE Learning, 2012.
7. Atul Kahate, *Cryptography and Network Security*, Mc Graw Hill, 3rd Edition, 2013
8. Bruce Schiener, *Applied Cryptography*, John Wiley & Sons, 1996
9. Neal Krawetz, *Introduction to Network Security*, CENGAGE Learning, 2007
10. Yang Xiao, Frank H Li, Hui Chen, *Handbook of Security of Networks*, World Scientific, 2011.