COURSE TITLE	**INFORMATION AND NETWORK SECURITY**
COURSE CODE	**01CE0613**
COURSE CREDITS	**3**

Objective:

1 The objective of Information and Network Security is to upgrade fundamentals of security over network. This course covers basic cryptography concepts, techniques and encryption algorithms.

Course Outcomes: After completion of this course, student will be able to:

1 Discover the fundamentals of symmetric cryptography, implement and analyse its methods, strengths, and flaws, from the viewpoint of cryptanalysis.

2 Implement and analyse various public key cryptography algorithms.

3 Discover the message authentication and its requirement, hashing idea and use different hashing algorithms to ensure the integrity of your messages.

4 Understand and use the message authentication and its requirement, the concepts of digital signature and digital certificates and various digital signature algorithms.

5 Understand and use the various key management and remote authentication mechanisms.

Pre-requisite of course:NA

Teaching and Examination Scheme

Theory Hours	Tutorial Hours	Practical Hours	ESE	IA	CSE	Viva	Term Work
2	0	2	50	30	20	25	25

Contents : Unit	Topics	Contact Hours
1	**Conventional Encryption and Techniques:** Conventional Encryption Model, Steganography, Classical Encryption Techniques, stream ciphers and block ciphers, Block Cipher structure, Data Encryption standard (DES), AES with structure, its transformationfunctions, key expansion, Multiple encryption and triple DES, Modes of Operations.	9
2	**Public Key Cryptography** Principles Of Public-Key Cryptography, RSA Algorithm, Diffie-Hellman Key Exchange	5
3	**Message Authentication, Hash Functions and Cryptographic Hash Functions** Authentication Requirement, Functions, Message Authentication Code, Hash Functions, MACs based on Hash Functions, Macs based on Block Ciphers. Cryptographic Hash Functions, Simple hash functions, its requirements and security, MD5 Message Digest Algorithm, Secure Hash Algorithm (SHA), HMAC.	6

MR. HARDIK AJAYBHAI DOSHI
Digitally signed by (Name of HOD)

DR. RAJENDRASINH BAHADURSINH JADEJA
Digitally signed by (Name of Dean/ Principal)

Contents : Unit	Topics	Contact Hours
4	**Digital Signature** Digital Signature, its properties, requirements and security, Digital Signature Standards, various digital signature schemes (Elgamal and Schnorr), NIST digital Signature algorithm.	5
5	**Network Security** Key management and distribution, Distribution of public keys, X.509 certificates, Kerberos.	2
Total Hours		**27**

Suggested List of Experiments:

Contents : Unit	Topics	Contact Hours
1	**Practical 1** Implement Caesar cipher encryption-decryption	2
2	**Practical 2** Implement Monoalphabetic cipher encryption-decryption.	2
3	**Practical 3** Implement Playfair cipher encryption-decryption.	2
4	**Practical 4** Implement Polyalphabetic cipher encryption-decryption.	2
5	**Practical 5** Implement Hill cipher encryption-decryption.	2
6	**Practical 6** Case Study on: Simple DES prepare report	2
7	**Practical 7** Case Study on: AES and prepare report	2
8	**Practical 8** Implement Diffi-Hellmen Key exchange Method.	2
9	**Practical 9** Implement RSA encryption-decryption algorithm.	2
10	**Practical 10** Write a program to generate SHA-1 hash.	2
11	**Practical 11** Implement a digital signature algorithm	2
12	**Practical 12** Perform various encryption-decryption techniques with cryptool.	2
13	**Practical 13** Study and use the Wireshark for the various network protocols.	2
Total Hours		**26**

Textbook :

1 Cryptography And Network Security Principles and Practice Fourth Edition, William Stallings,, Pearson Education., 2005

MR. HARDIK AJAYBHAI DOSHI
Digitally signed by (Name of HOD)

DR. RAJENDRASINH BAHADURSINH JADEJA
Digitally signed by (Name of Dean/ Principal)

References:

1 Modern Cryptography: Theory and Practice,, Modern Cryptography: Theory and Practice,, Wenbo Mao,, Prentice Hall PTR, 2003

2 Cryptography: Theory and Practice, Cryptography: Theory and Practice, Douglas R. Stinson, CRC press, 1995

3 Network Security: Private Communication in a Public World, Network Security: Private Communication in a Public World, Kaufman, R. Perlman, and M. Speciner,, Prentice Hall, 2002

Suggested Theory Distribution:

The suggested theory distribution as per Bloom's taxonomy is as follows. This distribution serves as guidelines for teachers and students to achieve effective teaching-learning process

Distribution of Theory for course delivery					
Remember / Knowledge	**Understand**	**Apply**	**Analyze**	**Evaluate**	**Higher order Thinking / Creative**
7.00	14.00	21.00	14.00	7.00	7.00

Instructional Method:

1 The course delivery method will depend upon the requirement of content and need of students. The teacher in addition to conventional teaching method by black board, may also use any of tools such as demonstration, role play, Quiz, brainstorming, MOOCs etc.

2 The internal evaluation will be done on the basis of continuous evaluation of students in the laboratory and class-room.

3 Practical examination will be conducted at the end of semester for evaluation of performance of students in laboratory.

4 Students will use supplementary resources such as online videos, NPTEL videos, e-courses, Virtual Laboratory.

Supplementary Resources:

1 http://cse29-iiith.virtual-labs.ac.in/exp8/index.php

MR. HARDIK AJAYBHAI DOSHI
Digitally signed by (Name of HOD)

DR. RAJENDRASINH BAHADURSINH JADEJA
Digitally signed by (Name of Dean/ Principal)