Uka Tarsadia University

C. G. Patel Institute of Technology

B. Tech.

Semester – 6

(030080602 / 030090602)

CRYPTOGRAPHY AND NETWORK SECURITY

EFFECTIVE FROM July-2017

Syllabus version: 1.02

Uka Tarsadia University

Version 1.02

SEMESTER-6
Cryptography and Network Security
(030080602/030090602)

Credits: 4 (Theory) **Contact hours per week: 4 (Theory)**

Objective of the course:

- To understand the fundamentals of cryptography
- To acquire knowledge on standard algorithm used to provide confidentiality, integrity and authenticity
- To understand various key distribution and management schemes
- To understand how to deploy encryption techniques to secure data in transit across network
- To design security applications in the field of IT

Student learning outcomes/objectives:

At the closing stage of the course, the student will be able

CO1	Analyze the vulnerabilities in any computing system
CO2	Be able to design various security solution
CO3	Identify the security issues in the network & resolve it
CO4	Evaluate security mechanisms using rigorous approaches including theoretical foundation
CO5	Evaluate security algorithms using mathematical foundation
CO6	Understand the basic design of the Security Algorithms

B. Tech.	Subject	Hours
Sem 6	030080602 / 030090602 Cryptography and Network Security	4 hrs/week
	(Theory)	4 Credits

Sr. No.	Topic	Hours
	Unit – I	
1	**Fundamentals of cryptography:** The OSI security architecture, Security attacks, Security services, Security mechanisms, A model for network security.	3
2	**Classical encryption techniques:** Symmetric cipher model, Substitution techniques, Transposition techniques, Steganography.	5
	Unit – II	
3	**Block ciphers:** Block Cipher Principles, Feistel cipher, Simplified DES, Data encryption standard, Strength of DES, Block cipher design principles, Multiple encryption and Triple DES.	11
	Unit – III	
4	**Number theory:** Modes of operations, Random number generation, Prime and relative prime numbers, Modular arithmetic, Euler's theorem, Euclid's algorithm.	7
5	**Confidentiality using symmetric encryption:** Traffic confidentiality, Key distribution.	4
	Unit – IV	
6	**Public key cryptography:** Principles of public key cryptosystems, RSA algorithm, Security of RSA, Key management, Diffie-Hellman key exchange.	11
	Unit – V	
7	**Message authentication and Hash function:** Authentication requirement, Authentication functions, Message authentication code and basic uses of message authentication code, Hash functions and basic uses of hash functions, Requirements of hash function, Message digest algorithm (MD5), Secure hash algorithm (SHA), HMAC.	5
8	**Digital Signatures and authentication protocols:** Digital signatures requirements, Digital signature standards, Kerberos.	3
	Unit – VI	

9	**Security at network layer:** IP security overview, IP security architecture, Encapsulating security payload, Authentication header.	4
10	**Security at transport layer:** Secure socket layer, Transport layer security, Secure electronic transaction.	4
11	**Security at application layer:** Pretty good privacy, S/MIME.	3

Practical
(030080602/030090602)
Cryptography and Network Security

Credits: 1 (Practical) **Contact Hours Per week: 2 (Practical)**

Sr. No.	Cryptography and Network Security (Practical)	Hours
1	Implementation of caesar cipher	2
2	Implementation of playfair cipher	4
3	Implementation of polyalphabetic cipher	2
4	Implementation of rail fence technique	2
5	Implementation of columnar technique	2
6	Implementation of RSA algorithm	4
7	Implementation of Diffie Hellman key exchange algorithm	4
8	Implementation of key generation for simplified DES	2
9	Implementation of encryption for simplified DES	4
10	Implementation of key generation for DES	4

Text book:

1. William Stallings - "Cryptography and Network Security" - 4th Edition, Pearson publication.

Reference books:

1. Behrouz Forouzan, Debdeep Mukhopadhyay – "Cryptography and Network Security", McGraw Hill education.
2. Dhiren Patel – "Information Security: Theory and Practice", PHI publication.
3. Atul Kahate – "Cryptography and Network Security", McGraw Hill education.
4. Bernard Menezes – "Network Security and Cryptography" – Cengage learning.

Course objectives and Course outcomes mapping:

- To understand the fundamentals of cryptography: CO1, CO2, CO5, CO6
- To acquire knowledge on standard algorithm used to provide confidentiality, integrity and authenticity: CO1, CO2, CO3, CO4, CO6
- To understand various key distribution and management schemes: CO2, CO4, CO6

- To understand how to deploy encryption techniques to secure data in transit across network: CO1, CO2, CO3, CO6
- To design security applications in the field of IT: CO1, CO2, CO3, CO6

Course units and Course outcome mapping:

Unit	CO1	CO2	CO3	CO4	CO5	CO6
Fundamentals of cryptography	√			√		√
Block ciphers		√				√
Number theory and issues in conventional cryptography		√			√	√
Public key cryptography		√		√	√	√
Message authentication and Hash function			√	√		√
Network security			√	√		√

Programme Outcomes:

- **PO 1: Engineering knowledge:** An ability to apply knowledge of mathematics, science, and engineering
- **PO 2: Problem analysis**: An ability to identify, formulates, and solves engineering problems
- **PO 3: Design/development of solutions**: An ability to design a system, component, or process to meet desired needs within realistic constraints
- **PO 4: Conduct investigations of complex problems**: An ability to use the techniques, skills, and modern engineering tools necessary for solving engineering problems.
- **PO 5: Modern tool usage**: The broad education and understanding of new engineering techniques necessary to solve engineering problems.
- **PO 6: The engineer and society:** Achieve professional success with an understanding and appreciation of ethical behavior, social responsibility, and diversity, both as individuals and in team environments.
- **PO 7: Environment and sustainability:** Articulate a comprehensive world view that integrates diverse approaches to sustainability.
- **PO 8: Ethics:** Identify and demonstrate knowledge of ethical values in non-classroom activities, such as service learning, internships, and field work.
- **PO 9: Individual and team work:** An ability to function effectively as an individual, and as a member or leader in diverse teams, and in multidisciplinary settings.
- **PO 10: Communication**: Communicate effectively on complex engineering activities with the engineering community and with society at large, such as, being able to comprehend and write effective reports and design documentation, make effective presentations, and give/receive clear instructions.
- **PO 11: Project management and finance**: An ability to demonstrate knowledge and understanding of the engineering and management principles and apply these to

one's own work, as a member and leader in a team, to manage projects and in multidisciplinary environments.

- **PO 12: Life-long learning:** A recognition of the need for, and an ability to engage in life-long learning.

Programme Outcomes and Course Outcomes mapping:

Programme Out come	Course out comes					
	CO1	CO2	CO3	CO4	CO5	CO6
PO1	√	√	√	√	√	√
PO2	-	-	√	√	√	-
PO3	√	√	√	√	-	√
PO4	√	-	√	√	√	-
PO5	√	√	√	√	-	√
PO6	-	-	-	-	-	-
PO7	-	-	-	-	-	-
PO8	-	-	-	-	-	-
PO9	√	√	√	√	√	√
PO10	-	-	-	-	-	-
PO11	√	√	√	√	√	√
PO12	√	√	√	√	√	√