Uka Tarsadia University

B. Tech.

Semester VI

CRYPTOGRAPHY

IT5018

EFFECTIVE FROM July-2021

Syllabus version: 1.00

Subject Code	Subject Title	Teaching Scheme			
		Hours		Credits	
		Theory	Practical	Theory	Practical
IT5018	Cryptography	4	2	4	1

Subject Code	Subject Title	Theory Examination Marks		Practical Examination Marks	Total Marks
		Internal	External	CIE	
IT5018	Cryptography	40	60	50	150

Objectives of the course:

- To explain the concept and mathematical background of cryptography.
- To illustrate the principles and design of cryptographic algorithms and protocols for achieving confidentiality, integrity and authentication in information security.
- To comprehend algorithms and protocols required for network and Internet security along with modern cryptographic concept.

Course outcomes:

Upon completion of the course, the student shall be able to

CO1: Understand the concept of computer security along with the mathematical background used in cryptography.
CO2: Evaluate and design various classical cryptography techniques and symmetric key cryptographic concepts.
CO3: Discuss and analyze the public key cryptography cryptosystems.
CO4: Understand the different hash function and digital signature scheme.
CO5: Differentiate and apply various OSI layer security and its protocols.
CO6: Understand the modern cryptographic and related technologies.

Sr. No.	Topics	Hours
	Unit – I	
1	**Introduction and Number Theory:** Computer security concepts, OSI security architecture, Security attacks, Services and mechanisms; Model for network security, Overview of prime numbers, Euclidean algorithm, Modular arithmetic, Euler's theorem, Euler's totient function, Fermat's theorem, Overview of group, Ring, Fields; Finite fields of the form GF(p), Polynomial arithmetic, Finite fields of the form GF(2^n), Random number generators.	9
	Unit – II	
2	**Classical Cryptography and Symmetric Key Cryptography:** Symmetric cipher model, Substitution techniques, Transposition techniques, Traditional block ciphers (SPN) - Feistel, Simplified Data Encryption Standard (DES), Block cipher design principles, Data Encryption Standard (DES), Multiple encryption and triple	12

	DES, Block cipher modes of operation, Advanced Encryption Standard (AES).	
Unit – III		
3	**Public Key Cryptography:** Principles of public key cryptosystems, RSA algorithm and its security, Key management with distribution of public keys, Diffie-Hellman key exchange, The El-Gamal cryptosystem and its security.	9
Unit – IV		
4	**Hash Functions and Digital Signature Scheme:** Introduction of hash functions, Applications of hash functions, Requirements and security, Secure Hash Algorithm (SHA), Message Authentication Codes (MAC) requirements and functions, MACs based on hash functions – HMAC; Digital signatures requirements, Digital signature standards, Digital Signature Algorithm (DSA).	12
Unit – V		
5	**Network and Internet Security:** Secure Socket Layer (SSL) architecture and working, Transport Level Security (TLS), Secure Shell (SSH) protocol, Pretty Good Privacy (PGP), S/MIME, IP Security, IPSec, IPSec Key Management.	10
Unit – VI		
6	**Modern Cryptographic Concepts:** Overview of crypto currencies and their architecture, Bitcoin and derivatives, Blockchain technology - Introduction, Features, Applications; Introduction of quantum cryptography and post-quantum cryptography.	8

Sr. No.	Cryptography (Practical)	Hours
1	Perform a practical to implement caesar cipher and play fair cipher.	4
2	Perform a practical to implement block chain network using bit coin core tool and demonstrate the bitcoin transaction on local network.	6
3	Perform a practical to install IPCOP firewall in Ubuntu and configure all its features.	4
4	Perform a practical to configure native VLAN using manageable switches using Cisco packet tracer for providing intranet security. c. Configure native VLAN on Cisco 2960 switches. d. Configure inter VLAN routing in Cisco packet tracer.	4
5	Perform a practical to configure TELNET and SSH using real devices and analyze packet flows and its payload using Wireshark.	4
6	Perform a practical to implement static and dynamic Network Address Translation (NAT) in Cisco packet tracer. Also perform NAT on Cisco 1941 series router.	4

7	Perform a practical to configure port address translation (PAT) in Cisco packet tracer.	4

Text Book:

1. William Stallings – "Cryptography and Network Security – Principles and Practice", Pearson Education.

Reference Books:

1. Forouzan and Mukhopadhyay – "Cryptography and Network Security", McGraw Hill, 2015.
2. Deven Shah – "Mark Stamp's Information Security Principles and Practice", Wiley-India.
3. Douglas Stinson – "Cryptography: Theory and Practice", Chapman & Hall.
4. Atul Kahate – "Cryptography and Network Security", McGraw Hill.
5. Bruce Schneier – "Applied Cryptography: Protocols, Algorithms and Source Code in C", John Wiley & Sons.

Course objectives and Course outcomes mapping:

- To explain the concept and mathematical background of cryptography: CO1, CO2
- To illustrate the principles and design of cryptographic algorithms and protocols for achieving confidentiality, integrity and authentication in information security: CO2, CO3, CO4
- To comprehend algorithms and protocols required for network and Internet security along with modern cryptographic concept: CO5, CO6

Course units and Course outcomes mapping:

Unit No.	Unit Name	Course Outcomes					
		CO1	CO2	CO3	CO4	CO5	CO6
1	Introduction and Number Theory	✓					
2	Classical Cryptography and Symmetric Key Cryptography		✓				
3	Public Key Cryptography			✓			
4	Hash Functions and Digital Signature Scheme				✓		
5	Network and Internet Security					✓	
6	Modern Cryptographic Concepts						✓

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 Outcomes	Course Outcomes					
	CO1	CO2	CO3	CO4	CO5	CO6
PO1	✓					
PO2		✓	✓	✓	✓	
PO3		✓	✓	✓	✓	✓
PO4		✓	✓	✓	✓	✓
PO5					✓	✓
PO6						
PO7						
PO8						
PO9						
PO10						
PO11						
PO12						