Uka Tarsadia University

B.Tech.

Semester V

INFORMATION SECURITY

CY5008

EFFECTIVE FROM June-2023

Syllabus version: 1.00

Subject Code	Subject Title	Teaching Scheme			
		Hours		Credits	
		Theory	Practical	Theory	Practical
CY5008	Information Security	3	2	3	1

Subject Code	Subject Title	Theory Examination Marks		Practical Examination Marks	Total Marks
		Internal	External	CIE	
CY5008	Information Security	40	60	50	150

Objectives of the course:

- To understand basic terminologies of Information security, correlate symmetric key cryptography and public key cryptography, usage of hash function and study basics of authentication methods and authorization.

Course Outcomes:

Upon completion of the course, the student will be able to:

CO1: Understand the basic terminologies of information security.

CO2: Understand symmetric key cryptography algorithms AES, DES, and Feistel cipher and Public key cryptography algorithm RSA, Diffie-Hellman

CO3: Comparative study of Symmetric and Public Key Cryptography algorithm.

CO4: Study basic concepts of hash function, Tiger hash and the birthday problem.

CO5: Understand types of authentication methods, storage and verification of passwords, and evaluate biometric applications based on the types of error rates.

CO6: Analyze basics of firewall and their classifications, CAPTCHA and its use and they shall predict types of intrusion detection technique based on a scenario.

Sr. No.	Topics	Hours
	Unit – I	
1	**Introduction of Information Security** Basics: Public key and Private Key, CIA: Confidentiality, Integrity, Availability, Terminologies of Cryptography, Classic Cryptography, History of Cryptography, Taxonomy of Cryptography, Taxonomy of Cryptanalysis	5
	Unit – II	
2	**Symmetric Key Cryptography** Stream Cipher: RC4, Block Cipher: ECB, CBC, IDEA, RC6, Blowfish,	6

	Feistel Cipher, DES, Triple DES, AES	
Unit – III		
3	**Public Key Cryptography** RSA, Diffie-Hellman, Public Key Notation, Use of Public Key Cryptography, Public Key Infrastructure	7
Unit – IV		
4	**Hash Functions** Hash Function and Use of Hash Function, The Birthday Problem, Non-Cryptographic Hashes, Tiger Hash, HMAC	7
Unit – V		
5	**Authentication** Authentication methods: Something you know, Something you are, Something You Have, Passwords, Password verification, Attacking Systems via passwords, Biometrics	6
Unit – VI		
6	**Firewall and Intrusion Detection** CAPTCHA, Introduction of Firewall, Classifications of Firewall, Personal Firewall, Intrusion Detection	5

Text book:

1. Deven Shah, “Mark Stamp’s Information Security Principles and Practice”, Wiley-India.

Reference books:

1. William Stalling, "Cryptography and Network Security", Pearson
2. Straub, Detmar W., Goodman, Seymour, Baskerville, Richard L, "Information Security : Policy, Processes, and Practices", PHI
3. Atul Kahate, "Cryptography and Network Security", McGraw Hill
4. David Bishop, "Introduction to Cryptography with Java Applets", Narosa Publishing House

Course objectives and Course outcomes mapping:

- Understand basic terminologies of Information security: CO1
- Compare different symmetric key cryptography and public key cryptography: CO2, CO3
- Study concepts of hash function: CO4
- Scrutinize basics of authentication and advanced concepts of authorization: CO5, CO6
- Understand basic terminologies of Information security: CO1

Course units and Course outcome mapping:

Unit No.	Unit Name	Course Outcomes					
		CO1	CO2	CO3	CO4	CO5	CO6
1	Introduction of Information Security	✓					
2	Symmetric Key Cryptography		✓				
3	Public Key Cryptography			✓			
4	Hash Functions				✓		
5	Authentication					✓	
6	Firewall and Intrusion Detection						✓

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						