GUJARAT TECHNOLOGICAL UNIVERSITY

BRANCH: CYBER SECURITY (59)

SUBJECT NAME: CRYPTOGRAPHY: PROTOCOLS AND STANDARDS

SUBJECT CODE: 2725909

SEMESTER: II

Type of course: Master of Engineering (Cyber Security)

Prerequisite: Cryptography fundamentals, ciphers

Rationale: Standard algorithms and protocols provide a focus for study; standards for popular applications provide specific structure for developing an application.

Teaching and Examination Scheme

Teaching Scheme			Credits	Examination Marks						Total Marks
				Theory Marks		Practical Marks				
L	T	P	C	ESE (E)	PA (M)	ESE (V)		PA (I)		
						ESE	OEP	PA	RP	
4	0	2	5	70	30	20	10	10	10	150

Content

Sr. No.	Content	Total Hours	%Weightage
1.	Protocol Building Blocks • Introduction to Protocols • Communications using Symmetric Cryptography • One-Way Functions • One-Way Hash Functions • Communications using Public-Key Cryptography • Digital Signatures • Digital Signatures with Encryption • Random and Pseudo-Random Sequence Generation	5	10%
2.	Basic Protocols • Key Exchange • Authentication • AUTHENTICATION AND KEY EXCHANGE • FORMAL ANALYSIS OF AUTHENTICATION AND KEY-EXCHANGE PROTOCOLS • Multiple-Key Public-Key Cryptography • Secret Splitting • Secret Sharing • Cryptographic Protection of Databases	5	10%
3.	Intermediate Protocols • Timestamping Services • Subliminal Channel • Undeniable Digital Signatures • DESIGNATED CONFIRMER SIGNATURES	8	30%

	• PROXY SIGNATURES • Group Signatures • Fail-Stop Digital Signatures • Computing with Encrypted Data • Bit Commitment • Fair Coin Flips • Mental Poker • ONE-WAY ACCUMULATORS • All-or-Nothing Disclosure of Secrets • KEY ESCROW		
4.	Advanced Protocols • ZERO-KNOWLEDGE PROOFS • Zero-Knowledge Proofs of Identity • Blind Signatures • IDENTITY-BASED PUBLIC-KEY CRYPTOGRAPHY • Oblivious Transfer • OBLIVIOUS SIGNATURES • Simultaneous Contract Signing • Digital Certified Mail • Simultaneous Exchange of Secrets	4	10%
5.	Esoteric Protocols • SECURE ELECTIONS • Secure Multiparty Computation • Anonymous Message Broadcast • DIGITAL CASH	3	5%
6.	Cryptography standards IPsec Virtual Private Network (VPN) IEEE P1363 Transport Layer Security (formerly SSL) SSH secure Telnet Content Scrambling System Kerberos authentication standard RADIUS authentication standard ANSI X9.59 electronic payment standard	11	35%

Suggested Specification table with Marks (Theory)

Distribution of Theory Marks					
R Level	U Level	A Level	N Level	E Level	C Level
10	**40**	**20**			

Legends: R: Remembrance; U: Understanding; A: Application, N: Analyze and E: Evaluate C: Create and above Levels (Revised Bloom's Taxonomy)

Note: This specification table shall be treated as a general guideline for students and teachers. The actual distribution of marks in the question paper may vary slightly from above table.

Reference Books

1. Everyday Cryptography:Fundamental principles and applications By Kevith M. Martin, Oxford University Press

2. Applied Cryptography: Protocols, Algorithms, and Source Code in C 2nd Edition by Bruce Schneier, WILEY

3. Companion to User's Guide to Cryptography and Standards, Alexander W. Dent Chris J. Mitchell,Amtech house

Course Outcome

After learning this course, the students should able to:

- Investigate protocols in cryptography.
- Apply standards in cryptography techniques.

List of Experiment

Full semester project can be taken up

1) Implement Kerberos authentication
2) Implement Radius authentication standards
3) Implement key exchange protocol
4) Implement certificate generation and certificate chaining.

Design based Problems (DP)/Open Ended Problem:

1) Develop a security protocol that fits for inter disciplinary engineering problem such as operating a high speed train.

Major Equipment:

Computer systems having following minimum technical configurations

Processor:i3 or i5 or higher

RAM: minimum 4 GB

HDD: 1 TB

Internet and Wi-Fi connectivity

License Window/Linux operating system