GUJARAT TECHNOLOGICAL UNIVERSITY

COMPUTER ENGINEERING (SYSTEMS AND NETWORK SECURITY) (56)

CRYPTOGRAPHY AND NETWORK SECURITY
SUBJECT CODE: 2715601
SEMESTER: I

Type of course: Foundation/Core

Prerequisite: Mathematical concepts: Random numbers, Number theory, finite fields

Rationale: The use of the Internet for various purpose including social, business, communication and other day to day activities has been in common place. The information exchanged through Internet plays vital role for their owners and the security of such information/data is of prime importance. Knowing the concepts, principles and mechanisms for providing security to the information/data is very important for the students of Computer Engineering/Information technology. The subject covers various important topics concern to information security like symmetric and asymmetric cryptography, hashing, message and user authentication, digital signatures, key distribution and overview of the malware technologies. The subject also covers the applications of all of these in real life applications.

Teaching Scheme:

Teaching Scheme			Credits	Examination Marks						Total Marks
L	T	P	C	Theory Marks		Practical Marks				
				ESE (E)	PA (M)	PA (V)		PA (I)		
						ESE	OEP	PA	RP	
3	2#	2	5	70	30	20	10	10	10	150

Sr. No.	Topic	Teaching Hours	Module Weightage
1	**Introduction** Understand basic Encryption Concepts: Symmetric Cipher Model, Cryptography, Cryptanalysis and Attacks; Substitution and Transposition techniques	2	10
2	**Symmetric Key Cryptography** Stream ciphers and block ciphers, Block Cipher structure, Feistel Cipher, Diffusion and Confusion, Data Encryption standard (DES) with example, strength of DES, Design principles of block cipher, AES, Multiple encryption and triple DES, Electronic Code Book, Cipher Block Chaining Mode, Cipher Feedback mode, Output Feedback mode, Counter mode, RC4 algorithm, Confidentiality using Symmetric encryption, Key Distribution, Random Number Generator	8	20
3	**Public Key Cryptography** Principles, RSA, Public Key Management, Deffie Helman Key Exchange, Elliptic Curve Cryptography	7	15

4	**Message Authentication and Hash Functions** Authentication Requirements, Authentication Functions, MAC, Hash Functions, Security of Hash Functions and MACs, SHA, MD5,	6	15
5	**Digital Signatures and Authentication Applications** Digital Signatures, Authentication Protocols, DSS, Kerberos, X.509, Public key Infrastructure.	3	10
6	**Email, IP and Web Security** PGP, S/MIME, IPSec Architecture, Authentication Header, ESP, Combining Security Association, Key Management, Web Security Consideration, SSL and TLS, Introduction to E-Commerce, Secure Electronic Transaction (SET).	4	10
7	**System Security** Intruders , Intrusion Detection, Virus and Worms, Virus Counter-Measures, DDOS attack, Firewall Design Principles, Trusted Systems.	3	10
8	**Other Security issues** Smart Cards and Security, Zero Knowledge Protocol, Enterprise Application Security, Biometric Authentication, Database Access Control, Security and Privacy Issues in RFIDs.	3	10

Reference Books:

1). William Stallings : "Cryptography and Network Security – Principles and Practice", 4/E, Pearson Education, 2005

2). Bruce Scheneir : "Applied Cryptography", 2/E, John Wiley,1996

3). Behrouz Forouzan : "Cryptography & Network Security", 1/E,TMH,2007

4). Menezes, Oorschot, Vanstone : "Handbook of Applied Cryptography", CRC Press,1996

5). D Stinson, "Cryptography: Theory and Practice", 2/E,Chapman & Hall ,2002

Course Outcome:

After learning the course, the students should be able to

1. Define the concepts of Information security and their use.
2. Describe the principles of symmetric and asymmetric cryptography.
3. Understand and apply the various symmetric key algorithms.
4. Understand and apply the various asymmetric key algorithms.
5. Understand the concepts of hashing with algorithms and apply them.
6. Understand and use the message authentication and its requirement.
7. Understand the concepts of digital signature and digital certificates.
8. List and explain various digital signature algorithms.
9. Understand and use the various key management and remote authentication mechanisms.
10. Understand the concept of malware technology and its impacts.

List of Experiments:

1. Implement en/decryption using Caesar cipher.

2. Implement en/decryption using Caesar Affine cipher.

[hint : $C = E([a,b], x) = (ax + b) \bmod 26$, where $\gcd(a,26) = 1$, and $0 < a, b < 26$]

3. Implement a program to perform letter frequency attack on given ciphertext and find out total frequency for each letter.
4. Implement en/decryption using Vigener cipher.
5. Implement en/decryption using 2 X 2 Hill cipher.
6. Implement en/decryption using Playfair cipher.
7. Implement en/decryption using Railfence cipher.
8. Implement en/decryption using Row Transposition cipher.
9. Implement steganography for hiding any kind of data using an image file. 11. Implement Euclidean Algorithm for finding GCD of two positive numbers.
12. Implement Extended Euclid for finding multiplicative inverse in GF(p).
13. Implement AES key expansion algorithm that takes 4 word [16 byte] key as input and produces 44 words that act as round keys for other rounds.
14. Implement MixColumns stage on given 4 X 4 state matrix for AES.
15. Implement RSA algorithm.
16. Implement Diffie-Hellman algorithm for key exchange.
17. Implement one-way hash function for storing password.
18. Write a program to generate SHA-1 hash.
19. Implement a digital signature algorithm.
20. Perform the various filtering operations using firewall software.

Open Ended Problems:

1. Study the standard document for the security policy for an organization and prepare the detailed security policy document for managing information security for your institute.
2. Develop a complete GUI based cryptography system using any symmetric key algorithm for practical use. Provide the performance analysis in terms of timing requirements.
3. Study the keytool provided by the Java to generate key pairs for public key cryptography.
4. Design and develop your own such tool to generate the key pair and test the pair with RSA implementation for encryption-decryption.
5. Simulate the complete system to act as key distribution centre for the distribution of the symmetric keys.
6. Develop a system to generate a digital certificate in X.509 format.
7. Study how the browsers manage the digital certificates for various secured websites for making secured communication.
8. Develop a system that detects the SQL injection attack on your database and prevent your database for such attack.
9. Configure the Active directory and DNS server for your organization to comply with security policy of the organization.

10. Check whether your browser supports security mechanism for phishing attack. If yes, provide the details that how your browser implements it.

Major Equipments:

- Latest PCs with related software

List of Open Source Software/learning website:

- Software: cryptool (www.cryptool.org)
- Software: snort (www.snort.org)
- Software: Wireshark (www.wireshark.org)
- http://www.cryptix.org/
- http://www.cryptocd.org/
- http://www.cryptopp.com/