GUJARAT TECHNOLOGICAL UNIVERSITY

CYBER SECURITY (59)
INTRODUCTION TO CRYPTOGRAPHY
SUBJECT CODE: 715903
SEMESTER: I

Type of course: Core

Prerequisite: Mathematical concepts: Random numbers, Number theory

Rationale:

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. The subject covers various important topics concern to information security like symmetric and asymmetric cryptography, hashing, message and user authentication, digital signatures and key management The Java Cryptography : Architecture and Extension is included.

Teaching and Examination Scheme:

Teaching Scheme			Credits	Examination Marks						Total Marks
L	T	P	C	Theory Marks		Practical Marks				
				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 HRS	% Weightage
1	**Introduction** : Need for Security, Approaches and Principles of security, Attacks **Cryptography Techniques** : Plain and Cipher text, Substitution and transposition technique, Encryption and Decryption, Symmetric and Asymmetric key cryptography, Key size and range, Possible attacks, DOS	5	10%
2	**Symmetric key cryptography algorithms** : Algorithm types and modes, DES, IDEA, RC4 and RC5 Blowfish, AES, Case Study	10	20%
3	**Asymmetric key cryptography algorithms** : History and Overview, RSA, Elgamal cryptography, Symmetric and Asymmetric, Digital signature, Knapsack algorithms, Elgamal digital signatures, Attacks, problems with public key exchange, Case study : virtual election	10	20%
4	**Public Key Infrastructure** : Digital certificates, Private key management, PKIX Model, PKCS, XML, PKI and security, case study: CSSV	5	10%
5	**User Authentication Mechanism** : Basics, Passwords, Authentication tokens, Certificate based and, Biometric authentication, Kerberos, KDC, Security handshake pitfalls, SSO, Attacks, Case Study : SSO	5	10%

6	**Java Cryptography** : Introduction to JCA and JCE, Provider, Security, SecureRandom, MessageDigest, Signature, Cipher, Mac classes and interfaces with their Application	10	20%
7	**Java Cryptography** : Key interface and classes with management Various Factory classes	5	10%
8	Application in modern research issues	2	-

Reference Books:

1. Cryptography and Network Security, 3rd Edition, Atul Kahate, TMH
2. Cryptography & Network Security, Forouzan, Mukhopadhyay, McGrawHill
3. Beginning Cryptography with Java, David Hook, Wrox
4. Cryptography And Network Security, Principles And Practice Sixth Edition, William Stallings, Pearson
5. Applied Cryptography, Bruice Schneier, Wiley
6. Information Systems Security, Godbole, Wiley-India
7. Information Security Principles and Practice, Deven Shah, Wiley-India
8. https://docs.oracle.com/javase/8/docs/technotes/guides/security/crypto/CryptoSpec.html
9. Build Your Own Security Lab : A Field Guide for network testing, Michael Gregg, Wiley India

Course Outcome:

After learning the course the students should be able to:.

- Describe the principles of symmetric and asymmetric cryptography.
- Understand and apply the various symmetric key algorithms.
- Understand and apply the various asymmetric key algorithms.
- Understand the concepts of hashing with algorithms and apply them.
- Understand and use the message authentication and its requirement.
- Understand the concepts of digital signature and digital certificates.
- List and explain various digital signature algorithms.
- Understand and use the various key management and remote authentication mechanisms. - Explore the Java Cryptography with their Application

List of Experiments:

- Minimum 10 experiments based on the contents.
  - Implementaion Symetrical Key Algorithm Such as
    - Substtition and Transcription Based Algo
    - S-Des implemenation
    - RSA Implemenation
    - Implemeation of Diffie-helman key Exchange
    - Implementation of symmetric Feistel Cipher Table algorithms
    - Implementation of Relative prime numbers
    - small firewall Implementation using TCP port based rule.
    - DES key generation algorithm
    - Signing a JAVA file using JAVA cryptograpgy API
    - Generating a Private and Public Key using JAVA API
    - Impelementation of descrete logarithms
    - Implementation of public/private key using of Elliptic curves
- Mini Project in a group of max. 3 students
- Writing a research paper on selected topic from content with latest research issues in that topic

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/

Review Presentation (RP): The concerned faculty member shall provide the list of peer reviewed Journals and Tier-I and Tier-II Conferences relating to the subject (or relating to the area of thesis for seminar) to the students in the beginning of the semester. The same list will be uploaded on GTU website during the first two weeks of the start of the semester. Every student or a group of students shall critically study 2 papers, integrate the details and make presentation in the last two weeks of the semester. The GTU marks entry portal will allow entry of marks only after uploading of the best 3 presentations. A unique id number will be generated only after uploading the presentations. Thereafter the entry of marks will be allowed. The best 3 presentations of each college will be uploaded on GTU website.