

GUJARAT TECHNOLOGICAL UNIVERSITY

Subject Name: PKI and Biometrics

Subject Code: 3725104

Semester: II

Type of course: M.E. Computer Engineering (IT systems and Network Security)

Prerequisite: Understanding of Cryptographic Algorithms and Key Infrastructure

Rationale: NA

Teaching and Examination Scheme:

Teaching Scheme			Credits C	Examination Marks				Total Marks
L	T	P		Theory Marks		Practical Marks		
				ESE (E)	PA (M)	ESE (V)	PA (I)	
3	2#	0	4	70	30	30	20	150

L- Lectures; T- Tutorial/Teacher Guided Student Activity; P- Practical; C- Credit; ESE- End Semester Examination; PA- Progressive Assessment;

Content:

Sr. No.	Content	Total Hrs	% Weightage
1	Understand Basic Encryption Concepts	2	4
2	Attacks Against Encryption	2	4
3	Understand Private Key Encryption Understand Public Key Encryption	2	4
4	Cryptography Fundamentals	2	4
5	Cryptographic Algorithm and protocols Symmetric Key Encryption Algorithms	2	4
6	Public Key Algorithms	2	4
7	Cryptographic issues	2	4
8	Strong Authentication Digital Signatures	2	4
9	PKI Standards PKI Fundamentals	2	4
10	Implementing Security	2	4
11	Understand Key Management Understand Trust in the System	2	4
12	Sign-On Solutions	2	4
13	Secure E-Mail Implementation,	2	4
14	File Encryption Solutions PKI Solutions and Applications	2	6
15	Legal Issues of Network Security	2	6
16	Introduction to Biometrics ,biometrics devices and techniques	3	6

Reference Books: - Cryptography & network Security: Principles And Practices, 4/e , William Stallings

- Implementing Biometric Security, John Chirillo Wiley
- Computer security basics, Rick Lehtinen, Deborah Russell, G. T. Gangemi
- Handbook of Biometrics, Springer's
- Introduction to biometrics, Anil k Jain, Springer's

Course Outcome:

After learning the course the students should be able to:

- Understand the cryptographic approach to security.
- Public and Private Key cryptography.
- Key Management for secure communication.
- Bio-metric systems to provide high level of security.
- Human Interactive approach to secure systems.

List of Experiments: (with Open Ended Problems)

- 1 Sniff packet using wireshark, dsniff and Cain and able
- 2 Working of bit locker in windows 7
- 3 Install and configure Data Recovery Agent
- 4 Install and Configure Truecrypt
- 5 Create SSH Connection without Password
- 6 CA using Auto enrolling and Web enrolling
- 7 Outlook Configure and issue mail certificate
- 8 Secure Mail Implementation using Thunderbird
- 9 Configure PGP and GPG in Linux
- 10 Configure Openssl in linux
- 11 Configure SSL in Apache2
- 12 Create Stunnel for secure comm...
- 13 SSLStrip use for catch Information
- 14 Configure Untangle and Working
- 15 Configure ClearOs and Working
- 16 Install and Configure Openvas
- 17 Install and Configure Nessus
- 18 Detail penetration test and solution using CVE of latest with detail description

Major Equipment:

- VMWare-Workstation
- Linux (Kali/Fedora/BT5/centOS)
- Windows Server 2008/2012
- Wireless Access Points
- Router
- Switches
- Bio-Metric Devices – Finger Print Reader
- Bio-Metric Devices – Face Detector
- IP Camera

List of Open Source Software/learning website:

- Linux

- OpenBDS
- OpenSwan
- VPN
- IPSec
- Metasploit
- www.schneier.com
- www.symantec.com/connect/blog
- www.cert-in.org.in

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.