GUJARAT TECHNOLOGICAL UNIVERSITY, AHMEDABAD, GUJARAT

COURSE CURRICULUM
COURSE TITLE: COMPUTER AND NETWORK SECURITY
(COURSE CODE: 3350704)

Diploma Programmes in which this course is offered	**Semester in which offered**
Computer Engineering	5th Semester

1. RATIONALE

Keep the system/data confidential, integrated and available is the prime concern of the current advanced digital world against various security threats which are increasing day by day. This demand for people working in security areas. This course aims that student should learn basic cryptography techniques and apply security mechanisms for measures for operating systems as well as private and public network. It will be also base for the group subject in the forthcoming semester.

2. COMPETENCY

The course content should be taught and implemented with the aim to develop different types of skills so that students are able to acquire following competency:

- Apply various cryptographic techniques and be able to determine appropriate mechanisms for protecting networked systems.

3. Course Outcomes:

i. Identify and describe the common types of security threats are risks to the Computer Systems and the nature of common Information hazards.
ii. Identify the potential threats to confidentiality, integrity and availability of Computer Systems.
iii. Describe the working of standard security mechanisms and applied to the external and internal network.
iv. Define cryptography, describe the elements of the encryption process and select best algorithm to encrypt data and protocols to achieve Computer Security.
v. Apply accepted security policies, procedures are necessary to secure Operating Systems and applications.

4. Teaching and Examination Scheme

Teaching Scheme (In Hours)			**Total Credits (L+T+P)**	**Examination Scheme**				
				Theory Marks		**Practical Marks**		**Total Marks**
L	**T**	**P**	**C**	**ESE**	**PA**	**ESE**	**PA**	**200**
3	**0**	**4**	**7**	**70**	**30**	**40**	**60**	

Legends: **L**-Lecture; **T** – Tutorial/Teacher Guided Theory Practice; **P** - Practical; **C** – Credit **ESE** - End Semester Examination; **PA** - Progressive Assessment**.**

5. COURSE DETAILS

Unit	Major Learning Outcomes	Topics and Sub-topics
Unit – I Introduction and Security Threats:	1a.Define Various security terms. 1b. List various Threats. 1c. Define Security Basics.	1.1 Threats to security : Viruses and Worms, Intruders, Insiders, Criminal organizations, Terrorists, Information warfare 1.2 Security Basics – Confidentiality, Integrity, Availability 1.3 Types of attack: Denial of service (DOS), backdoors and trapdoors, sniffing, spoofing, man in the middle, replay, TCP/IP Hacking, Phishing attacks, Distributed DOS, SQL Injection. Malware : Viruses, Logic bombs
Unit – II Organizational Security	2a.List & Define various human security threats. 2b. List potential threats on password and explain characteristics of a strong password.	2.1 Password selection, Piggybacking, Shoulder surfing, Dumpster diving, Installing unauthorized software /hardware, Access by non employees, 2.2 Security awareness, Individual user responsibilities. 2.3 Password Management, vulnerability of password, password protection, password selection strategies, components of a good password.
Unit – III Cryptography and Public key Infrastructure	3a. List various Symmetric Encryption Algorithms. 3b. Explain various encryption Algorithms. 3c. Explain Hashing. 3d. Distinguish Asymmetric and Symmetric Encryption. 3e. Distinguish public key & private key Infrastructure. 3f. Explain Digital Signature & Digital Certificate.	3.1 Introduction to Symmetric encryption & Asymmetric encryption, 3.2 Encryption algorithm / Cipher, Caesar’s cipher, playfair cipher, hill cipher (using small matrix and encryption only), shift cipher, verman cipher, one time pad, Vigenere cipher. 3.3 Transposition techniques (rail fence), Steganography 3.4 Introduction to Hashing :

Unit	Major Learning Outcomes	Topics and Sub-topics
		definition, block diagram and characteristics of good hash function, applications 3.5 Public key infrastructures : basics, digital signatures, digital certificates, certificate authorities, registration authorities, steps for obtaining a digital certificate, steps for verifying authenticity and integrity of a certificate 3.6 Centralized or decentralized infrastructure, private key protection
Unit IV Network security	4a. Explain working principle of FIREWALLs. 4b.Define various security topologies. 4c. Explain email security.	4.1 Firewalls: Types of Firewall, Personal Firewall, Network Firewall, Software Firewall, Hardware Firewall, Packet Filtering Firewall, working, design principles, trusted systems, Kerberos. 4.2 Security topologies – security zones, DMZ, Internet, Intranet, VLAN, security implication, tunneling. 4.3 Email security : security of email transmission, malicious code, spam, mail encryption
Unit V Web Security	5a. Define & list various IDSs. 5b. Distinguish Host-based IDS & Network-based IDS. 5c.List & Explain Web Security Threats.	5.1 Intruders, Intruder Behavior Patterns, Intrusion Techniques Intrusion detection systems (IDS) : host based IDS, network based IDS. 5.2 Web Trafficking & it’s Analysis. 5.3 Web security threats, web traffic security approaches, Introduction to SSL & TLS, Concepts of secure electronic transaction

6. SUGGESTED SPECIFICATION TABLE WITH HOURS & MARKS (THEORY)

Unit No.	Unit Title	Teaching Hours	Distribution of Theory Marks			
			R Level	U Level	A Level	Total Marks
I	Introduction and Security Threats	6	4	4	4	12
II	Basics of System Security	6	4	4	4	12
III	Cryptography and Public key Infrastructure	14	6	8	8	22
IV	Network security	8	2	4	6	12
V	Web Security	8	2	4	6	12
	Total	**42**	**18**	**24**	**28**	**70**

Legends: R = Remembrance; U = Understanding; A = Application 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.

7. SUGGESTED LIST OF EXERCISES/PRACTICALS

S. No.	Unit No.	**Practical Exercises** (Outcomes' in Psychomotor Domain)	Hrs. required
1	I	List and practice various "net" Commands on DOS & Linux.	04
2	I	Configure a system for various security experiments.	02
3	I	Configure Web browser security settings.	02
4	I	Draw Diagram of DoS, backdoors, trapdoors.	04
5	I & II	Draw diagrams of sniffing, spoofing, man in the middle & replay attacks.	02
6	I	Draw diagram for Confidentiality, Integrity & Availability.	02
7	III	Write Ceaser's Cipher algorithm & Solve various examples based on Encryption & Decryption.	02
8	III	Write, test and debug Ceaser cipher algorithm in C/C++/Java/Python/Matlab.	02
9	III	Write algorithm/steps for Shift Cipher & solve various examples on it.	02
10	III	Write algorithm/steps for Hill Cipher and solve	02

		examples on it.	
11	III	Write algorithm/steps for playfair cipher and solve examples on it.	02
12	III	Write algorithm/steps for Verman Cipher & solve various examples on it.	02
13	III	Write algorithm/steps for Vignere Cipher & solve various examples on it.	02
14	III	Write algorithm/steps for one time pad & solve various examples on in.	02
11	III	Draw diagram of Public Key Infrastructure.	02
12	III	Draw diagram of Centralized/Decentralized Infrastructure.	02
13	III	Demonstrate cross-scripting.	02
14	IV	Draw various Security Topologies.	02
15	IV	Demonstrate traffic analysis of different network protocols using tool. i.e. Wire-shark. (Atleast one of them should be recorded and included in term work.)	04
16	IV	Demonstrate Sniffing using packet tool i.e. snort.	04
17	IV	Configure your e-mail account against various threats. i.e. spam attack, phising, spoofing etc.	04
18	V	Draw diagram Host-based Intrusion Detection System	02
19	V	Draw diagram Network-based Intrusion Detection System	02
20	V	Demonstration of SQL-Injection.	02
21	V	Demonstration of readymade encryption/decryption code	04
Total			**62**

8. SUGGESTED LIST OF STUDENT ACTIVITIES

Following is the list of proposed student activities like:

i. Visit to Internet Service Provider

ii. Study measures are taken by small computer industries

iii. Seminars on various security tools, algorithms from the course content

iv. Seminars on current threats on system/network

9. SPECIAL INSTRUCTIONAL STRATEGIES (if any)

The course activities include Lectures and Practical Exercises as per teaching scheme. The programmes in would be executed during practical’s sessions. Following needs attention:

i. Concepts will be introduced in lectures using multimedia projector.
ii. Discussion
iii. Demonstrations
iv. Power point presentation for each of the software tools/algorithms
v. Practical work will be through laboratory sessions.
vi. Debate/Group Discussions for comparison of various tools and algorithms

10. SUGGESTED LEARNING RESOURCES

A) List of Books

S.No.	Title of Book	Author	Publication
1.	Cryptography and Network Security Principal and Practices	Atul Kahate	Tata-McGraw-Hill Sixth reprint 2006
2.	Cryptography and Network Security Principles and Practices	Williams Stallings	Pearson Education, Third Edition
3.	Cryptography and Network Security	B A Forouzen	TMH
4.	Computer Security Basics	Deborah Russell G.T.Gangenisr	O'Reilly publication
5.	Computer Security	Dieter Gollman	Wiley India Education, Second Edition

B) List of Major Equipment/ Instrument with Broad Specifications

i. Computer System with latest configuration and memory, laptops, servers
ii. Multimedia projector
iii. High B/W Internet Connection.
iv. Open source Free diagnostic software/tools
v. Access to library resources

C) List of Software/Learning Websites

i. Software: Wireshark Traffic Analysis/Packet Sniffing Tool, Snort Packet Sniffing tool
ii. http://mercury.webster.edu/aleshunas/COSC%205130/COSC%205130%20Home.htm
iii. http://williamstallings.com/Cryptography/
iv. http://mercury.webster.edu/aleshunas/COSC%205130/Chapter-22.pdf
v. http://nptel.iitm.ac.in/courses.php?disciplineId=106
vi. Network Simulator Tool: GNS3 v0.8.5, NetSimK
vii. http://www.snort.org/docs
viii. http://manual.snort.org/node27.html
ix. http://www.wireshark.org/docs/wsug_html_chunked/
x. http://www.pearsonhighered.com/assets/hip/us/hip_us_pearsonhighered/samplechapter/0131407333.pdf
xi. http://www.cs.nyu.edu/courses/fall04/G22.2262-001/assignments/assignment4_files/Ethereal_TCP.pdf

11. COURSE CURRICULUM DEVELOPMENT COMMITTEE

Faculty Members from Polytechnics

- **Prof. P. P. Kotak, H. O. D., Computer Department, A. V. P. T. I., Rajkot**
- **Prof. K. N. Raval, H.O.D Computer Department, R. C. Technical Institute, Ahmedabad**
- **Prof. Manisha P Mehta, Sr. Lecturer in Computer Technology, K. D. Polytechnic, Patan.**
- **Prof. Sunil R. Solanki, Lecturer in Computer Engineering, Govt. Polytechnic, Dahod.**
- **Prof. Sachin D. Shah, Lecturer in Computer Engineering, R. C. Technical Institute, Ahmedabad.**

Coordinator and Faculty Members from NITTTR Bhopal

- **Dr. M. A. Rizvi, Associate Professor, Dept. of Computer Engineering and Applications.**
- **Dr. R. K. Kapoor, Associate Professor, Dept. of Computer Engineering and Applications, NITTTR**