GUJARAT TECHNOLOGICAL UNIVERSITY, AHMEDABAD, GUJARAT

COURSE CURRICULUM
COURSE TITLE: WEB AND NETWORK SECURITY
(COURSE CODE: 3361601)

Diploma Program in which this course is offered	Semester in which offered
Information Technology	SIXTH

1. RATIONALE

The objective of the course is to enable the students to understand about the advances in network and web security. It covers the basic underlying concepts and techniques recently being used in the IT industry. After going through this course students will be able to understand public key cryptography as well as digital signature. They will also learn about various encryption algorithms using public key cryptography. They will also appreciate significant security mechanisms being employed for network and web security. Thus this course is an important course for IT engineers.

2. COMPETENCIES

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 competencies:

- **Manage various Encryption Algorithms for Web Security Applications**
- **Apply Network security**

3. COURSE OUTCOMES:

The theory should be taught and practical should be carried out in such a manner that students are able to acquire different learning out comes in cognitive, psychomotor and affective domain to demonstrate following course outcomes.

i. Describe importance of RSA Algorithm and Asymmetric cryptography.
ii. Explain Basic concept of Message Authentication Codes
iii. Explain basic concept of Web Security.
iv. Demonstrate use of digital signature
v. Apply Application level security on web browser
vi. Apply various parameters of antivirus and firewall security on network.

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	150
4	0	2	6	70	30	20	30	

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

5. COURSE DETAILS

Unit	Major Learning Outcomes (in cognitive domain)	Topics and Sub-topics
Unit – I **Public Key Crypto Systems**	1a. Describe the basics of Asymmetric cryptography	1.1 Asymmetric key cryptography: History and its overview
	1b. Explain the principles Of Public-Key Cryptosystems	1.2 Principles of pubic key cryptosystems. 1.2.1 Simplified working of public key cryptosystem: Secrecy. 1.2.2 Simplified working of public key cryptosystem: Authentication. 1.2.3 Simplified working of public key cryptosystem: Secrecy and Authentication. 1.3 Applications of Public Key cryptosystems. 1.4 Requirements for Public-Key Cryptography 1.5 Public-Key Cryptanalysis
	1c. Describe RSA Algorithm, its approach ,block diagram and security aspects	1.6 RSA algorithm: Description and explanation 1.7 General approach, block diagram and example for RSA. 1.8 The Security of RSA
Unit – II **MAC and Hash Functions**	2a. Explain Hash Functions , MD5 and basics of SHA	2.1 Applications of cryptographic Hash Functions. 2.2 Hash function based on block ciphers.(Block diagram and explanation only) 2.2.1 Rabin scheme. 2.3 Message Digest5 Hashing 2.4 Requirements for a cryptographic Hash function. 2.5 Secure Hash Algorithm (SHA) its overview. 2.5.1 Comparison of SHA parameters
	2b. Describe Message Authentication Code	2.6 Message Authentication: Requirements and Functions 2.6.1 Message Encryption 2.7 Message Authentication Code: Introduction and Requirements 2.8 Security of MAC 2.8.1 Brute-Force Attacks 2.8.2 Cryptanalysis
Unit – III **Network Security Application**	3a. Describe applications of Digital Signature. 3b.Demonstrate use of digital signature	3.1 Digital signatures: Definition and Properties. 3.1.1 Difference between conventional and digital signature. 3.1.2 Digital signature requirements and Applications. 3.2 Digital Signature Standard (DSS) Approach 3.3 Applications of Digital signatures.
	3b. Explain PGP and S/MIME Electronic Mail Security	3.4 Pretty Good Privacy(PGP): Operational Description, Confidentiality and Authentication, General format of PGP message

		3.5 S/MIME 3.5.1 MIME contents types.: 3.5.2 S/MIME functions:Concept,Introduction
	3c. Explain IP Security	3.6 IP Security Overview 3.6.1 Applications and benefits of IPsec. 3.6.2 IPsec documents. 3.6.3 IPsec Services.
Unit – IV **Web Security**	4a. Explain Web Security	4.1 Web Security Considerations. 4.1.1 Web security threats. 4.1.2 Web traffic security approaches. 4.2 Secure Socket Layer and Transport Layer Security 4.2.1 Overview of SSL Protocol Stack(diagram and explanation only) 4.3 HTTPS 4.3.1 Connection initiation. 4.3.2 Connection closure.
	4b. Apply Application level security on web browser	4.4 Basic Concept of Secure Electronic Transactions 4.5 SSL versus SET 4.6 D Secure Protocol
Unit - V **System Security**	5a. Explain Intrusion, Intrusion detection techniques and password management. 5b.Install and Configure an Antivirus Software	5.1 Intrusion 5.2 Classification of Intruders 5.3 Intrusion Detection techniques. 5.3.1 Statistical anomaly detection 5.3.2 Rule based detection. 5.4 Password Management 5.4.1 Password selection strategies. 5.5 Malicious software : Virus and Related Threats, Virus Countermeasures
	5c.Install and configure Firewall	5.6 Need of firewall. 5.7 Firewall characteristics. 5.8 Types of Firewall 5.8.1 Packet filtering firewall. 5.8.2 Application proxy firewall. 5.8.3 Circuit level proxy firewall.

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	**Public Key Crypto Systems**	08	2	8	0	10
II	**MAC and Hash Functions**	12	4	8	4	16
III	**Network Security Application**	16	6	6	4	16
IV	**Web Security**	10	4	6	4	14
V	**System Security**	10	2	6	6	14
	Total	**56**	**18**	**34**	**18**	**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/PRACTICAL

The practical/exercises should be properly designed and implemented with an attempt to develop different types of skills **(outcomes in psychomotor and affective domain)** so that students are able to acquire the competencies/programme outcomes. Following is the list of practical exercises for guidance.

***Note**: Here only outcomes in psychomotor domain are listed as practical/exercises. However, if these practical/exercises are completed appropriately, they would also lead to development of certain outcomes in affective domain which would in turn lead to development of **Course Outcomes** related to affective domain. Thus over all development of **Programme Outcomes (**as given in a common list at the beginning of curriculum document for this programme) would be assured.*

Sr. No.	**Unit No.**	**Practical Exercises** (Outcomes in Psychomotor Domain)	**Hrs. required**
1	I	Prepare a 5 slides presentation of RSA, explaining its working and structure	02
2	II	1. Generate an executable file from a C compiler and generate its Message Digest Sum (MD5) sum. Note down the MD5. 2. Change the above C program with a minor modification and again generate its executable. Check the MD5 of the new file. Verify the MD5 of both the files. 3. Take 5 different application executables and check their MD5 in similar manner. Reference : (www.md5summer.org/download.html). You can alternatively use online MD5 generator.	02
3	II	1. Generate an executable file from a C compiler and generate is Secure Hash Algorithm (SHA-256, SHA-512) sum. Note down the SHA values. 2. Change the above C program with a minor modification and again generate its executable. Check the SHA 256 and 512 of the new file. Verify the SHA values of both the files. 3. Take 5 different application executables and check their SHA values. Reference: (http://www.xorbin.com/tools/sha256-hash-calculator). You can download the desktop based SHA generator	02
4	II	Prepare a chart/model Message Authentication Codes(MACs)	02
5	III	Prepare a chart /model to explain the importance of Digital Signature	02
6	III	Install Wireshark tool for packet capture.	02
7	III	Inspect IP packets and identify source and destination IP using the wireshark tool	02
6	IV	Prepare a Chart and/or presentation on SSL Protocol Stack.	02
8		1. Download Avast free AV or Clam AV open source. Check the updates of the anti malware.	04

		2. Identify you operating system. Update the OS and identify updates.	
9		Prepare a presentation on 3D authentication for monetary transactions (SET)	02
10	V	Install and configure an Antivirus for Network security	04
11		Install and configure few features of Firewall for Network security	04
12	V	Inspect the firewall at your department in CWN. Understand its functionality, identify the important configuration parameters for the same.	04
		(Total Practical Hours)	**34**
NOTE: Perform any of the practical exercises for total minimum of 28 hours from above list depending upon the availability of resources so that skills required for most of the outcomes in the all units are developed.			

8. SUGGESTED LIST OF STUDENT ACTIVITIES

Following is the list of proposed student activities such as:

- Seminar (student would prepare seminar on security features adopted by some reputed companies/banks etc to protect their websites and data)
- Students would use power point presentations in above seminar and there would be group discussions on the strengths and weakness of the security features adopted by the concern company.

9. SPECIAL INSTRUCTIONAL STRATEGIES (if any)

i. Concepts should be introduced in classroom input sessions and by giving demonstration through projector.

ii. Arrange expert lectures by IT experts working for security of websites and data of some reputed financial company or bank etc.

iii. More focus should be given on practical work which will be carried out in laboratory sessions. If possible some theory sessions may be conducted in labs so that theory and practice can go hand in hand.

iv. Application for practical will be assigned to the students by the subject faculty and Students will work in a group of 3 maximum.

v. Group Discussion and presentation of relevant websites

vi. Faculty should allow students to use their creativity and let them struggle to learn on their own during practical sessions. However, faculty should remain around the students and should help them when they are stuck. Assignment can be given based on above topics.

10. SUGGESTED LEARNING RESOURCES

A) List of Books

S. No.	Title of Book	Author	Publication
1	Cryptography and Network Security	William Stallings	Pearson

2	Cryptography and Network Security	Forouzon	Mc Graw Hill
3	Network Security Essentials.	William Stallings	Pearson
4	Network Security: Private Communication in a Public World	CharlieKaufman	Prentice Hall
5	Cryptography Theory and Practice	Douglas R. Stinson	

B) **List of Software/Learning Websites**

- Download MD5 Application www.md5summer.org/download.html
- Download Wireshark Tools https://www.wireshark.org/tools/
- SecTools.Org: Top 125 Network Security Tools http://sectools.org/
- SHA-256 hash calculator http://www.xorbin.com/tools/sha256-hash-calculator
- Firewall Analyzer http://www.manageengine.com/products/firewall/?gclid=CO_Zh4DwtcICFYUrjgodx1cA9g&gclsrc=aw.ds

Electronic Teaching Slides (Power Point Slides)- CD/DVD

- RSA
- PKCS
- PGP
- Digital Signature
- Firewall

Laboratory Charts

- Asymmetric key Encryption
- Authentication
- DSS approach

11. COURSE CURRICULUM DEVELOPMENT COMMITTEE

Faculty Members from Polytechnics

i). **Prof. Manoj Parmar ,Incharge Head(IT),G P Himmatnagar.**
ii). **Prof. Manish D. Patel, Incharge Head (IT), RCTI,Ahmedabad.**
iii). **Mr. Sunil Paryani, Lecturer (IT), G P Himmatnagar.**
iv). **Ms. Darshna M. Trivedi,Lecturer (IT), RCTI Ahmedabad.**

Coordinator and Faculty Members from NITTTR Bhopal

- **Dr.K.James Mathai,** Associate Professor, Department of Computer Engineering & Applications.
- **Prof (Mrs.) Priyanka Tripathi,** Associate Professor, Department of Computer Engineering & Applications.