GUJARAT TECHNOLOGICAL UNIVERSITY, AHMEDABAD, GUJARAT

COURSE CURRICULUM
COURSE TITLE: ESSENTIALS OF NETWORK SECURITY
(COURSE CODE: 3351602)

Diploma Program in which this course is offered	Semester in which offered
Information Technology	5th Semester

1. RATIONALE

The objective of Information Security is to upgrade fundamentals of security over network. This course covers basic cryptography concepts, techniques and encryption algorithms. After going through this course student will be able to configure security policy in OS.

2. LIST OF COMPETENCY

The course content should be taught and implemented with the aim to develop required f skills in students so that they are able to acquire following competencies:

- **Explain basics of Information Security.**
- **Identify and explain functioning of various Encryption Algorithms.**
- **Apply the security techniques for information protection.**

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 Security in Communication.
ii. Explain basic concept of Encryption Algorithm.
iii. Elaborate Firewall Techniques.
iv. Explain latest trends in OS Security Assessment Tools.
v. Install various firewalls for information security.
vi. Apply/Use anti malware and Cleanup Tools for betterment of information security.
vii. Apply/Use antivirus effectively for the security of OS.

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 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 **Introduction of Information Security**	1a. Explain basic concepts related to Information Security	1.1 Need of Information Security 1.2 Security Trends 1.3 What is Information Security 1.4 Overview of Information Security 1.5 Security Services 1.6 Security Mechanism 1.7 Security Attacks 1.8 The OSI Security Architecture 1.9 A Model for Network Security
Unit – II **System Security**	2a. Define Symmetric Key and Cryptography	2.1 Symmetric Cipher Model 2.2 Cryptography 2.3 Cryptanalysis
	2b. Define Classical Encryption Techniques. 2c. Identify various ciphers techniques available. 2d. Define steganography along with its usage.	2.4 Substitution Techniques 2.4.1 Caesar Cipher 2.4.2 Monoalphabetic Cipher 2.4.3 Polyalphabetic Cipher 2.4.4 Playfair Cipher 2.4.5 Hill Cipher 2.5 Problems with Symmetric Cipher Algorithms 2.6 Diffie-Hellman Key exchange algorithm 2.5 Transposition Techniques 2.6 Steganography
Unit – III Basic Arithmetics in Encryption	3a. Describe basic concept in Number theory and finite fields	3.1 Divisibility and The Division Algorithm 3.2 The Euclidean Algorithm 3.3 Modular Arithmetic 3.4 Random Number 3.4 Groups, Rings, and Fields 3.5 Finite Fields of the Form GF(p)
Unit – IV Symmetric Encryption Algorithm	4a. Discuss Block Cipher principle.	4.1 Block Cipher Principal
	4b. Define data encryption standards commonly used. 4c. Identify Block cipher modes of	4.2 The Data Encryption Standard 4.3 Fiestel Structure 4.4 First Round of DES 4.5 Strength of DES 4.5.1 Double DES 4.5.2 Man in the Middle Attack

Unit	Major Learning Outcomes (in cognitive domain)	Topics and Sub-topics
	operations available.	4.6 Block Cipher Modes of Operation 4.6.1 Electronic Code Book 4.6.2 Cipher Block Chaining Mode 4.6.3 Cipher Feedback Mode 4.6.4 Output Feedback Mode 4.6.5 Counter Mode
Unit - V Asymmetric Key Encryption	5a. State the limitations of symmetric encryption	5.1 Limitations of Symmetric Key Encryption
	5b. Describe asymmetric key encryption. 5c. Identify confidentiality and authentication.	5.2 Asymmetric Key Encryption 5.2.1 Maintaining Confidentiality 5.2.2 Maintaining Authentication 5.2.3 Managing confidentiality and authentication together
Unit- VI Operating System Security	6a. Configure different firewalls for OS security.	6.1 Windows OS Hardening 6.1.1 Configure Security Policy 6.1.2 Configure Firewall (Win XP, Win 7)
	6b. Describe antivirus approaches available. 6c. Use antivirus available for the information security.	6.2 Anti Malware and Cleanup Tools 6.2.1 Windows AVG 6.2.2 ClamAV (Open source) 6.2.3 Avast
	6d. Use the security assessment tools on different OS viz. Windows, Linux.	6.3 OS Security Assessment Tools 6.3.1 Nessus (Windows, Linux) 6.3.2 SAINT (Linux, Open Source)
	6e. Describe the importance of OS updates. 6f. Use updates available in open source for different operation systems.	6.4 OS Updates 6.4.1 Windows Patches 6.4.2 Windows Upgrades 6.4.3 Linux Updates, upgrades

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 of Information Security	05	4	4	2	10
II	System Security	12	4	6	6	16
III	Basic Arithmetic in Encryption	05	2	2	4	08
IV	Symmetric Encryption Algorithm	10	4	4	8	16
V	Asymmetric Key Encryption	05	2	4	4	10
VI	Operating System Security	05	2	4	4	10
	Total	**42**	**18**	**24**	**28**	**70**

Legends: R = Remember; U = Understand; A = Apply and above levels (Bloom's Revised 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.*

Faculty should refer to that common list and should ensure that students also acquire outcomes in affective domain which are required for overall achievement of Programme Outcomes/Course Outcomes.

Sr. No.	Unit No.	Practical Exercises (Outcomes in Psychomotor Domain)	Hrs. required
1	I	Prepare report on various security trends and security services.	4
2		Prepare report on various security attacks and security mechanism.	2
3		Prepare report on OSI Security Architecture.	2
4	II	Prepare report on various cryptographic technique.	4
5		Prepare report on cryptanalysis.	4
6	III	Perform encryption of a plain text and decryption of cipher text using one time pad method	4
7		Perform encryption of plain text and decryption of cipher text of a using caesar cipher.	4

Sr. No.	Unit No.	Practical Exercises (Outcomes in Psychomotor Domain)	Hrs. required
8		Perform encryption of a plain text and decryption of cipher text using Monoaplhabetic cipher.	4
9		Perform encryption of a plain text and decryption of cipher text using play fair cipher.	2
10		Perform decryption of a cipher text using polyalphabetic cipher	2
11		Perform encryption of a plain text and decryption of cipher text using rectangular cipher	4
12		Perform encryption of a plain text and decryption of cipher text using columnar cipher	4
13		Perform encryption of a plain text and decryption of cipher text using Hill cipher	4
14	IV	Prepare report on block cipher modes of operation.	2
15		Prepare report on single round of DES.	2
16	V	Prepare report on Asymmetric encryption.	2
17	VI	Configure Security in OS (Win XP / Win 7)	4
18		Configure firewall of (Winx XP/ Win 7)	4
Total Hours			58

8. SUGGESTED LIST OF STUDENT ACTIVITIES

Following is the list of proposed student activities such as:

i. Seminar with power point presentation

ii. Configure firewall on a network.

iii. Design a model of Network Security

9. SPECIAL INSTRUCTIONAL STRATEGIES (if any)

Assignment can be given based on above topics. Students should be allowed to work on their own and show their creativity, faculty should provide help only when students have tried their best.

10. SUGGESTED LEARNING RESOURCES

A) List of Books

S. No.	Title of Book	Author	Publication
1	Cryptography and Network Security: Principles and Practice	William Stallings	Prentice Hall
2	Cryptography: An Introduction	Nigel Smart	Mcgraw-Hill College
3	Cryptography and Network Security	Forouzan	McGraw Hill
4	Network Security Essentials	William Stallings	Pearson
5	Network Security Tools: Writing, Hacking, and Modifying Security Tools	Justin Clarke, Nitesh Dhanjani	O'Reilly Media;

	- See more		
6	Network Security	Atul Kahate	Tata McGraw Hill
7	Cryptography and Security in Computing	Jaydip Sen	In Tech

B) List of major equipment with major Specification

- Desktop computer P-IV processor or higher
- LINUX

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

- Data Encryption Standard
- Feistel Structure
- Block cipher modes of Opeartion

Laboratory Charts

- Security Attacks
- Security Mechanisms
- OSI Security Architecture

C) List of Software/Learning Websites

i. www.**cryptography**.com
ii. **http://searchsecurity.techtarget.com**
iii. cse.iitkgp.ac.in/

11. COURSE CURRICULUM DEVELOPMENT COMMITTEE

Faculty Members from Polytechnics

- **Prof Parvez K. Faruki,** In charge Head (IT), BPTI, Bhavnagar
- **Prof Manoj P. Parmar,** In charge Head (IT), G. P. Himatnagar.
- **Prof. Manish D. Patel ,** In charge Head (IT), R C T I Ahmedabad
- **Prof Sunil Paryani,** Lecturer , IT , G P Himatnagar
- **Prof (Ms.) Darshana Trivedi,** Lecturer, IT, RCTI, Ahmedabad

Coordinator and Faculty Members from NITTTR Bhopal

- **Dr. M. A. Rizvi,** Associate Professor, Dept. of Computer Engineering and Applications.
- **Dr. Priyanka Tripathi**, Associate Professor, Dept. of Computer Engineering and Applications, NITTTR.