22IT510 INFORMATION SECURITY

Category	L	T	P	Credit
PCC	3	0	0	3

Preamble

This course on Information Security focuses on the models, tools, and techniques for enforcement of security with emphasis on the use of cryptography. Upon completion of the course, the learners will be able to develop basic understanding of security, cryptography, system attacks and defences against them.

Prerequisite

Nil

Course Outcomes

On the successful completion of the course, students will be able to

COs	Course Outcomes	TCE Proficiency Scale	Expected Proficiency in %	Expected Attainment Level %
CO1	Perform Encryption/ Decryption of text using symmetric and asymmetric crypto algorithms to provide confidentiality.	TPS3	80	65
CO2	Compute hash and digital signature for the given message to provide integrity and non-repudiation service.	TPS3	80	65
CO3	Examine the strength of any cryptographic algorithm by cryptanalysis.	TPS3	70	60
CO4	Explain different types of authentication and key agreement protocols.	TPS2	90	75
CO5	Use security protocols such as SSL, IP Sec etc., at different layers of TCP/IP stack to develop security solutions	TPS3	80	65
CO6	Identify security attacks and vulnerabilities in any information system and provide preventive measures and solutions in adherence with security standards	TPS4	70	60

Mapping with Programme Outcomes and Programme Specific Outcomes

COs	PO1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO 10	PO 11	PO 12	PS O1	PS O2	PS O3
CO1	S	M	L		L								M		
CO2	S	M	L		L								M		
CO3	S	S	M	L	L								S		
CO4	M	L											M		
CO5	S	M	L										M		
CO6	S	S	M	L	M			S	M	M		S	S	M	M

S- Strong; M-Medium; L-Low

Assessment Pattern

CO	CAT1				Assignment 1				CAT2				Assignment 2				Terminal			
	100				100				100				100				100			
TPS Scale	**1**	**2**	**3**	**4**	**1**	**2**	**3**	**4**	**1**	**2**	**3**	**4**	**1**	**2**	**3**	**4**	**1**	**2**	**3**	**4**
CO1	8	8	34				50											10	30	
CO2			16				25											5	10	
CO3	9	9		16				25				18								10
CO4									16									10		
CO5									16	16	16				50			5	10	
CO6												18				50				10

***** Terminal examination should cover all Course Outcomes in the appropriate TPS Scale level.

Syllabus

Basics of Information Security – Perspectives and Impact, Threats and vulnerabilities, Attacks, Security Services -CIA Triad and Security Models, Internet Law and Cyber Crimes, Security Standards

Cryptography - Mathematics for Cryptography – Number Theory - Modulo Arithmetic - Euclidean and extended Euclidean Theorem - Chinese Remainder Theorem - Euler and Fermat theorem, Galois Fields, Primality Testing Methods

Symmetric Key Cryptosystems –Hill Cipher, Advanced Encryption Standard, Public Key Cryptography - RSA , Elliptic Curve Cryptosystems , Integrity – Message Authentication Code and Hash , Application of Hash in Blockchain Technologies, Digital Signatures.

Authentication and Key Exchange – One way Authentication- Mutual Authentication- Dictionary Attacks- Kerberos- Biometrics- Multifactor Authentication. Key management – Digital certificates- Public Key Infrastructure.

Security Protocols Security at Application Layer – PGP, Electronic Payments – SET Security at Transport Layer –SSL and TLS, Security at Network layer –IP Sec

Network Defense Tools - Firewalls, Intrusion Prevention and Detection Systems.

Secure Software Development -Software Vulnerabilities – OWASP Web Application Security Concerns -Phishing, Buffer Overflows, Format String Attacks, Cross Site Scripting, SQL injection, DoS, DDoS, Session Hijacking and Pharming Attacks.

Non cryptographic Protocol Vulnerabilities –Viruses, Worms and Malwares -Case Studies

Text Book

1. Behrouz. A. Foruzan and Debdeep Mukhopadhyay, “Cryptography and Network Security”, Tata McGraw Hill , Third Edition, 2016.

Reference Books & web resources

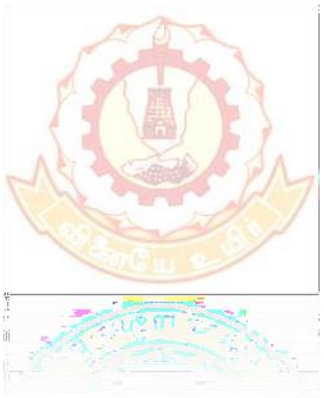
1. William Stallings, “Cryptography and Network Security: Principles and Practice”, Prentice Hall,Seventh Edition, 2017.
2. Bernard L Menezes, and Ravinder Kumar “Cryptography, Network Security and Cyber Laws”, Cengage Learning India Pvt Limited, 2018.
3. Charlie Kaufman and Radia Perlman, Mike Speciner, “Network Security, Private Communication in Public World”, Prentice Hall India, Second Edition, 2002.
4. William Stallings, "Network Security Essentials: Applications and Standards", Prentice Hall, Sixth Edition, 2016.
5. Man Young Rhee, "Internet Security Cryptographic Principles, Algorithms and Protocols", Wiley, First Edition, 2003.
6. Douglas R. Stinson, “Cryptography Theory and Practice”, Third Edition, Chapman & Hall/CRC, 2006.
7. https://onlinecourses.nptel.ac.in/noc22_cs90/preview

Course Contents and Lecture Schedule

Module No.	Topic	No. of Periods
1	**Basics of Information Security**	
1.1	Perspectives and Impact, Threats and vulnerabilities, Attacks, Security Services -CIA Triad and Security Models, Internet Law and Cyber Crimes, Security Standards	2
2	**Cryptography**	
2.1 2.2 2.3	**Mathematics for Cryptography – Number Theory** Modulo Arithmetic Euclidean and extended Euclidean Theorem, Chinese Remainder Theorem	2
2.4	Galois Fields	2
2.5 2.6	Euler and Fermat theorem Primality Testing Methods	1
2.7	**Symmetric Key Cryptosystems** –Hill Cipher	2
2.8	Advanced Encryption Standard	3
2.9	**Public Key Cryptography** - RSA	2
2.10	Elliptic Curve Cryptosystems	2
2.11	Integrity – Message Authentication Code and Hash	2
2.12	Application of Hash in Blockchain Technologies,	1
2.13	Digital Signatures	1
3	**Authentication and Key Exchange**	
3.1 3.2 3.3	One way Authentication Mutual Authentication Passwords and Dictionary Attacks	1
3.4	Biometrics- Multifactor Authentication	1
3.5 3.6	**Key management** Digital certificates Public Key Infrastructure	2
4	**Security Protocols**	
4.1	Security at Application Layer – PGP, Electronic Payments- SET	2
4.2	Security at Transport Layer –SSL and TLS,	1
4.3	SET Security at Network layer –IP Sec	1
5	**Network Defense Tools**	
5.1	Firewalls	1
5.2	Intrusion Prevention and Detection Systems	1
6	**Secure Software Development** OWASP Web Application Security Concerns	
6.1 6.2 6.3	Phishing Buffer Overflows Format String Attacks	1
6.4	Cross Site Scripting	1
6.5 6.6	SQL injection, DoS and DDoS	1
6.7 6.8	Session Hijacking Pharming Attacks	1
7	**Non cryptographic Protocol Vulnerabilities**	
7.1 7.2 7.3	Viruses Worms Malwares Case Studies	2
	Total	36

Course Designer(s):

1. Jeyamala.C, Associate Professor, jeyamala@tce.edu, Information Technology
2. Parkavi.R, Assistant Professor, rpit@tce.edu, Information Technology



22IT570	INFORMATION SECURITY LAB

Category	L	T	P	Credit
PCC	0	0	2	1

Preamble

The laboratory course on Information security aims to provide hands on experience in using various crypto libraries for securing computer applications. Practical exposure on usage of various network security tools for analyzing security vulnerabilities and protection is provided.

Prerequisite

None

Course Outcomes

On the successful completion of the course, students will be able to

COs	Course Outcomes	TCE Proficiency Scale	Expected Proficiency in %	Expected Attainment Level %
CO1	Utilize symmetric and public key cryptography to offer confidentiality in simple application development	TPS3	80	70
CO2	Perform message and entity authentication using hashing and digital signatures	TPS3	80	70
CO3	Use standard crypto libraries for crypt analysis	TPS4	80	70
CO4	Configure and manage network defense tools like Firewalls and Intrusion Detection Systems	TPS3	80	70
CO5	Identify software vulnerabilities such as SQL injection and provide solutions for prevention and detection	TPS4	80	70
CO6	Analyze the network attacks and identify the malwares in the network	TPS4	80	70

Mapping with Programme Outcomes

COs	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3
CO1	S	M	L		M			M	L			M	M	M	L
CO2	S	M	L		M			M	L			M	M	M	L
CO3	S	S	M	L	M			M	L			M	S	M	L
CO4	S	M	L		M			M	L			M	M	M	L
CO5	S	S	M	L	M			M	L	L		M	S	M	L
CO6	S	S	M	L	M			M	L	L		M	S	M	L

S- Strong; M-Medium; L-Low

Assessment Pattern

Cognitive Levels	Model Examination	Terminal Examination
Remember		
Understand		
Apply	60	60
Analyse	40	40
Evaluate		
Create		

.

Course Contents

Ex. No.	Topic	No. of Sessions	COs
1	Implementation and Crypt analysis of Hill Cipher	1	CO1/CO3
2	Develop a secure client server communication using symmetric key algorithms (Use Standard crypto Libraries)	1	CO1/CO3
3	Implement RSA cryptosystem with key management	1	CO1/CO3
4	Verify integrity of client server communication using Hashing techniques	1	CO2
5	Perform Man in the middle attack in Diffie Hellman Key Exchange protocol	1	CO1
6	Perform password extraction, cracking and recovery from target system	1	CO4
7	Simulation of SQL Injection attack - Testing Web applications for SQL injection vulnerabilities, Scanning web servers, analyzing logs, Securing web application	1	CO5
8	Configuration of Firewalls in system environment / using OPNET or Cisco Packet Tracer or GNS3	1	CO4
9	Simulation of Virtual Private Network using OPNET or Cisco Packet Tracer or GNS3	1	CO4
10	Study of Transport Layer Security Protocol using Wireshark	1	CO4
11	Configure Intrusion Detection System tool for monitoring events in a host to detect malicious activities	1	CO4
12	Creation, Detection and Prevention of Buffer overflow attack, Cross site scripting	1	CO6
	Total Sessions	**12**	

Course Designer(s):

1. Dr.C.Jeyamala, Associate Professor, Department of IT jeyamala@tce.edu
2. Mrs.R.Parkavi, Assistant Professor, Department of IT rpit@tce.edu