Lesson Plan

Branch: Computer Engineering
Semester: VI **Year: 2022-23**

Course Title: Cryptography and System Security (CSC602)	SEE: 3 Hours – Theory
Total Contact Hours: 36 Hours	Duration of SEE: 3 Hrs
SEE Marks: 80 (Theory) + 20 (IA)	
Lesson Plan Author: Prof. Monali Shetty	Date: 5-1-23
Checked By:	Date: 9-1-23

Prerequisites: Computer Networks

Syllabus:

Module		Content	Hrs
1		**Introduction - Number Theory and Basic Cryptography**	**8**
	1.1	Security Goals, Attacks, Services and Mechanisms, Techniques. Modular Arithmetic: Euclidean Algorithm, Fermat's and Euler's theorem	
	1.2	Classical Encryption techniques, Symmetric cipher model, mono-alphabetic and polyalphabetic substitution techniques: Vigenère cipher, Playfair cipher, Hill cipher, transposition techniques: keyed and keyless transposition ciphers	
2		**Symmetric and Asymmetric key Cryptography and key Management**	**11**
	2.1	Block cipher principles, block cipher modes of operation, DES, Double DES, Triple DES, Advanced Encryption Standard (AES), Stream Ciphers: RC4 algorithm.	
	2.2	Public key cryptography: Principles of public key cryptosystems- The RSA Cryptosystem, The knapsack cryptosystem	
	2.3	Symmetric Key Distribution: KDC, Needham-Schroeder protocol. Kerberos: Kerberos Authentication protocol, Symmetric key agreement: Diffie Hellman, Public key Distribution: Digital Certificate: X.509, PKI	
3		**Cryptographic Hash Functions**	**3**
	3.1	Cryptographic hash functions, Properties of secure hash function, MD5, SHA-1, MAC, HMAC, CMAC.	
4		**Authentication Protocols & Digital Signature Schemes**	**5**
	4.1	User Authentication, Entity Authentication: Password Base, Challenge Response Based	
	4.1	User Authentication, Entity Authentication: Password Base, Challenge Response Based	
5		**Network Security and Applications**	**9**
	5.1	Network security basics: TCP/IP vulnerabilities (Layer wise), Network Attacks: Packet Sniffing, ARP spoofing, port scanning, IP spoofing	
	5.2	Denial of Service: DOS attacks, ICMP flood, SYN flood, UDP flood, Distributed Denial of Service	
	5.3	Internet Security Protocols: PGP, SSL, IPSEC. Network security: IDS, Firewalls	
6		**System Security**	**3**
	6.1	Buffer Overflow, malicious Programs: Worms and Viruses, SQL injection	

Course Outcomes (CO):

On successful completion of course learner will be able to:

CSC602.1. Explain system security goals and its concepts, acquire and apply knowledge on the concepts of modular arithmetic and number theory to classical encryption techniques.

CSC602.2. Describe and compare different techniques for encryption, decryption and, authentication.

CSC602.3. Discuss various hash functions, digital signature algorithms to verify integrity and their cryptanalysis.

CSC602.4. Discuss various attacks on network security, and the security protocols.

CSC602.5. Differentiate between various malicious programs.

CO-PO Mapping: (BL – Blooms Taxonomy, C – Competency, PI – Performance Indicator)

CO	BL	C	PI	PO	Mapping
CSC602.1.	1, 2, 3	1.3	1.3.1	PO1	1
CSC602.2.	2, 4	1.3	1.3.1	PO1	1
		2.2	2.2.4	PO2	1
CSC602.3.	2	1.3 1.4	1.3.1 1.4.1	PO1	2
CSC602.4.	2	1.3 1.4	1.3.1 1.4.1	PO1	2
		6.1	6.1.1	PO6	1
CSC602.5.	4	1.3 1.4	1.3.1 1.4.1	PO1	2

	PO1	**PO2**	**PO3**	**PO4**	**PO5**	**PO6**	**PO7**	**PO8**	**PO9**	**PO10**	**PO11**	**PO12**
CSC602.1	1											
CSC602.2	1	1										
CSC602.3	2											
CSC602.4	2					1						
CSC602.5	2											

CO-PSO Mapping:

CO	BL	C	PI	PO	Mapping
CSC602.4.	2	2.2 2.3 2.4	2.2.2 2.3.1 2.4.1	PSO2	2

	PSO1	PSO2
CSC602.1.	--	--
CSC602.2.	--	--
CSC602.3.	--	--
CSC602.4.	--	3
CSC602.5.	--	--

Competencies and PIs for POs	
1.3 Demonstrate competence in engineering fundamentals	1.3.1 Apply engineering fundamentals
1.4 Demonstrate competence in specialized engineering knowledge to the program	1.4.1 Apply theory and principles of Computer Science and engineering to solve an engineering problem
2.2 Demonstrate an ability to formulate a solution plan and methodology for an engineering problem	2.2.4 Compare and contrast alternative solution/methods to select the best methods
6.1 Demonstrate an ability to describe engineering roles in a broader context, e.g. pertaining to the environment, health, safety, legal and public welfare	6.1.1 Identify and describe various engineering roles; particularly as pertains to protection of the public and public interest at the global, regional and local level
Competencies and PIs for PSOs	
2.2 Demonstrate an ability to identify potential threats and attacks to the information technology assets.	2.2.2 Identify the flow and methodology of the attacks.
2.3 Demonstrate an ability to identify tools and measures to protect the assets from cyber-attacks.	2.3.1 Identify the defence methodologies and the measures to prevent the attacks and protect assets.
2.4 Demonstrate an ability to apply the security mechanisms to real-world problems.	2.4.1 Simulate the solution on a virtual system.

CO Measurement Weightages for Tools:

Course Outcomes	***Direct Method (80%)***								***Indirect Method (20%)***
	Unit Tests		Assignments			Quizzes		End Sem Exam	Course exit survey
	1	2	1	2	3	1	2		
CSC602.1	10%	--	20%	--	--	10%	--	60%	100%
CSC602.2	20%	--	--	10%	--	10%	--	60%	100%
CSC602.3	10%	10%	--	--	10%	--	10%	60%	100%
CSC602.4	--	10%	--	--	20%	--	10%	60%	100%
CSC602.5	--	10%	--	--	20%	--	10%	60%	100%

Attainment:

CO CSC602.1:

Direct Method

$$A_{\text{CSC602.1}D} = 0.1 * Test1 + 0.2 * Assignment + 0.1 * Quizzes + 0.6 * SEE\_Theory$$

Final Attainment:

$$A_{\text{CSC602.1}} = 0.8 * A_{\text{CSC602.1}D} + 0.2 * A_{\text{CSC602.1}I}$$

CO CSC602.2:
Direct Method

$$A_{\text{CSC602.2}D} = 0.2 * Test1 + 0.1 * Assignment + 0.1 * Quizzes + 0.6 * SEE\_Theory$$

Final Attainment:

$$A_{\text{CSC602.2}} = 0.8 * A_{\text{CSC602.2}D} + 0.2 * A_{\text{CSC602.2}I}$$

CO CSC602.3:
Direct Method

$$A_{\text{CSC602.3}D} = 0.1 * Test1 + 0.1 * Test2 + 0.1 * Assignment + 0.1 * Quizzes + 0.6 * SEE\_Theory$$

Final Attainment:

$$A_{\text{CSC602.3}} = 0.8 * A_{\text{CSC602.3}D} + 0.2 * A_{\text{CSC602.3}I}$$

CO CSC602.4:
Direct Method

$$A_{\text{CSC602.4}D} = 0.1 * Test2 + 0.2 * Assignment + 0.1 * Quizzes + 0.6 * SEE\_Theory$$

Final Attainment:

$$A_{\text{CSC602.4}} = 0.8 * A_{\text{CSC602.4}D} + 0.2 * A_{\text{CSC602.4}I}$$

CO CSC602.5:
Direct Method

$$A_{\text{CSC602.5}D} = 0.1 * Test2 + 0.2 * Assignment + 0.1 * Quizzes + 0.6 * SEE\_Theory$$

Final Attainment:

$$A_{\text{CSC602.5}} = 0.8 * A_{\text{CSC602.5}D} + 0.2 * A_{\text{CSC602.5}I}$$

Course Level Gap (if any): Nil

Content beyond Syllabus:

Guest Lecture on Real Time Deployment and Applications of Blockchain in Industry.

Lecture Plan:

Module	Contents	Hours	Planned date	Actual date	Content Delivery Method	Remark
1	Introduction, vulnerabilities, threats, attacks; Security goals, attacks	8	9-1-23	9-01-23	PPT	
	Security services, mechanisms, Techniques, Euclidean algorithm		10-1	10-01-23	PPT	
	Modular Arithmatic, Extended Euclidean algorithm		13-1	11-01-23	PPT & Board	
	Fermat's thm, Eulers thm, additive, multiplicative inverse, Chinese Remainder thm		17-1	16-01-23	PPT & Board	
	Cryptanalytic attacks, Classical encryption techniques: intro, Substitution cipher: Additive, Multiplicative, Affine cipher		18-1	17-01-23	PPT (online)	
	Playfair cipher, Vigenère cipher		21-1	23-01-23	PPT & Board	
	Hill Cipher		24-1	24-01-23	PPT + Board	
	Transposition ciphers: keyed, keyless		25-1	27-01-23	Board	
2	RSA cryptosystem, Principles of public key cryptography	15	27-1	30-01-23	PPT & Board	Assignment 1 on module 1
	Knapsack cryptosystem		30-1	31-01-23	Board	
	Block cipher Principles: Feistel cipher		31-1	03-02-23	PPT	
	Data Encryption Standard (DES): Encryption, decryption		3-2	06-02-23	PPT	
	Avalanche effect, strengths of DES, Double DES		6-2	07-02-23	Board	
	Tripple DES: with two keys, with three keys, Man-in-the-Middle attack, known-plaintext attack		7-2	10-02-23	PPT & Board	
	Advanced Encryption Standard (AES)		10-2	13-02-23	PPT	
	AES		13-2	14-02-23	PPT	
	Block cipher modes: Electronic Code Book, Cipher Block Chaining mode		14-2	15-02-23	PPT	
	Cipher feedback mode, output feedback mode, counter mode		17-2	-	Self study	
	RC4 Algorithm		20-2	17-02-23	PPT(Online)	
	KDC, Needham-Schroeder protocol		21-2	20-02-23	PPT(Online)	
	Kerberos: Kerberos Authentication protocol		24-2	21-02-23	PPT (Online)	UT1: 28/02/23 to 03/03/23
	Diffie-Hellman key exchange, Man-in-the-Middle attack		27-2	24-02-23	PPT & Board	
	Digital Certificate: X.509, PKI		6-3	27-2-23	PPT	Assignment 2 on module 2
3	Properties of secure hash function, MD-5, SHA-1 algorithm	2	7-3	10-3	PPT	Quiz 1 on module 1&2

	MAC, HMAC, CMAC			13-3	PPT	
4	User Authentication: Password Based	4	10-3	17-3	PPT	
	Challenge Response Based		13-3	17-3	PPT	
	Digital signature scheme: RSA		17-3	Lab	Demo, implemetation	
5	Network security basics: TCP/IP vulnerabilities	6	20-3	20-3	PPT	
	Network Attacks: Packet Sniffing, ARP spoofing, port scanning, IP spoofing		21-3	21-3	PPT	
	DOS attacks, ICMP flood, SYN flood,		24-3	Lab	Lab	Assignment 3 on module 3 to 6
	UDP flood, Distributed Denial of Service, Internet Security Protocols: PGP		27-3	24-3	PPT	
	SSL, IPSEC		3-4	27-3	PPT + Board	Quiz 2 on module 3 to 6
	Network security: IDS, Firewalls		4-4	3-4	PPT	28-3, 31-3 Euphoria
6	Buffer Overflow	3	7-4		Self-Study	(4-4 , 7-4 H)
	Malicious Programs: Worms and Viruses		10-4	10-4	PPT	
	SQL injection		11-4	11-4	PPT	

Text books:

1. William Stallings, ***"Cryptography and Network Security, Principles and Practice"***, 6th Edition, Pearson Education, March 2013.
2. Behrouz A. Ferouzan, ***"Cryptography & Network Security"***, Tata McGraw Hill.
3. Behrouz A. Forouzan & Debdeep Mukhopadhyay, ***"Cryptography and Network Security"*** 3rd Edition, McGraw Hill.

Reference Books:

1. Bruce Schneier, ***"Applied Cryptography, Protocols Algorithms and Source Code in C",*** Second Edition, Wiley.
2. Atul Kahate, ***"Cryptography and Network Security",*** Tata McGraw-Hill Education, 2003.
3. Eric Cole, ***"Network Security Bible",*** Second Edition, Wiley, 2011.

Web References:

1. https://github.com/cmin764/cmiN/blob/master/FII/L3/SI/book/W.Stallings%20-%20Cryptography%20and%20Network%20Security%206th%20ed.pdf
2. https://docs.google.com/file/d/0B5F6yMKYDUbrYXE4X1ZCUHpLNnc/view

Evaluation Scheme

CIE Scheme

Internal Assessment: 20 (Average of two tests)

Internal Assessment Scheme

Module		Lecture Hours	No. of questions in		No. of questions in SEE
			Test 1	Test 2	
1	Introduction - Number Theory and Basic Cryptography	8	01 (5 marks)	--	3
2	Symmetric and Asymmetric key Cryptography and key Management	11	02 (5 Marks each)	--	4/5
3	Cryptographic Hash Functions	6	01 (5 Marks)	01 (5 Marks)	1
4	Authentication Protocols & Digital Signature Schemes	10	--	01 (5 Marks)	2
5	Network Security and Applications	12	--	01 (5 Marks)	4
6	System Security	4	--	01 (5 Marks)	1

Note: Four to six questions will be set in the Test paper

Verified by:

Programme Coordinator Subject Expert