CRYPTOGRAPHY AND NETWORK SECURITY (Th. 01)

Date of Commencement of classes: 14.03.2022 **Date of Closing of classes:** 11.06.2022

LIST OF WEEK/ MONTH WISE AVAILABLE DAYS/ PERIODS

Sl. No.	Month	Week-wise no. of academic days available					Total no. of academic days
		Week- 1	Week- 2	Week- 3	Week- 4	Week- 5	
1	March	--	--	4	6	3	13
2	April	2	5	4	4	6	21
3	May	5	4	4	5	2	20
4	June	3	6	--	--	--	09
Total		**10**	**15**	**12**	**15**	**11**	**63**

NO. OF AVAILABLE CLASSES PER WEEK/ MONTH

Sl. No.	Month	Week-wise no. of academic periods available					Total no. of academic periods
		Week- 1	Week- 2	Week- 3	Week- 4	Week- 5	
1	March	--	--	4	6	3	13
2	April	2	5	4	4	6	21
3	May	5	4	4	5	2	20
4	June	3	6	--	--	--	09
Total		**10**	**15**	**12**	**15**	**11**	**63**

TOPIC-WISE DISTRIBUTION OF PERIODS

Sl. No.	Name of the Chapter	Periods as per Syllabus	Required period	Expected Marks
01	POSSIBLE ATTACKS ON COMPUTERS	05	06	20
02	CRYPTOGRAPHY CONCEPTS	10	10	20
03	SYMMETRIC & ASYMMETRIC KEY ALGORITHMS	15	13	20
04	DIGITAL CERTIFICATE & PUBLIC KEY INFRASTRUCTURE	10	08	15
05	INTERNET SECURITY PROTOCOLS	10	08	10
06	USER AUTHENTICATION	04	07	15
07	NETWORK SECURITY & VPN	06	06	10
TOTAL		**60**	**58**	**110**

Sign of Lect. **Sign of HOD.** **Sign of AIC** **Sign of Vice Principal**

LESSON PLAN

Name of the Month	Week No.	Class day	Art. No.	Theory Topics
MARCH	3rd	1st	1.1	**Chapter No.- 01(Possible Attacks On Computers)** The need for security
		2nd	1.2	Security approach
		3rd	1.3	Principles of security
		4th		Continue…….
	4th	1st	1.4	Types of attacks
		2nd		Continue….
		3rd	2.1	**Chapter No.- 02 (Cryptography Concepts)** Plain text & Cipher Text
		4th	2.2	Substitution techniques
		5th		Cont.
		6th	2.3	Transposition techniques
	5th	1st		Continue
		2nd	2.4	Encryption & Decryption
		3rd	2.5	Symmetric key cryptography
APRIL	1st	1st		Asymmetric key cryptography
		2nd		Continue
	2nd	1st		Symmetric & Asymmetric key cryptography difference
		2nd	3.1	**Chapter No.- 03 (Symmetric & Asymmetric Key Algorithms)** Symmetric key algorithm types
		3rd		Continue…….
		4th	3.2	Overview of Symmetric key cryptography
		5th		Continue….
	3rd	1st	3.3	Data encryption standards
		2nd	3.4	Over view of Asymmetric key cryptography
		3rd		Continue…
		4th	3.5	The RSA algorithm
	4th	1st		Problem using RSA algorithm
		2nd		Problem
		3rd	3.6	Symmetric key cryptography
		4th		Asymmetric key cryptography
	5th	1st	3.7	Digital signature
		2nd	4.1	**Chapter No.- 04(Digital Certificate & Public Key Infrastructure)** Digital certificates
		3rd		Continue…
		4th	4.2	Private key management
		5th		Continue
		6th	4.3	PKIX Model
	1st	1st		Continue
		2nd	4.4	Public key cryptography standards
		3rd		Continue…

M A Y		4th	5.1	**Chapter No.- 05(Internet Security Protocols)** Basic concept
		5th		Secure socket layer
	2nd	1st	5.2	Continue…
		2nd	5.3	Transport layer security
		3rd	5.4	Secure Hypertext transfer protocol (SHTTP)
		4th		Continue…
	3rd	1st	5.5	Time stamping protocol (TSP)
		2nd	5.6	Secure electronic transaction (SET)
		3rd	6.1	**Chapter No.- 06(User authentication)** Authentication basics
		4th	6.2	Password
	4th	1st	6.3	Authentication Tokens
		2nd		Continue
		3rd	6.4	Certificate based authentication
		4th		Continue
		5th	6.5	Biometric authentication
	5th	1st	7.1	**Chapter No.- 07(Network Security & VPN)** Brief introduction of TCP/IP
		2nd		Continue
J U N E	1st	1st	7.2	Firewall
		2nd	7.3	IP Security
		3rd		Continue
	2nd	1st	7.4	Virtual Private Network (VPN)
		2nd	Ch-01	Revision-1/Previous yr Question Answer discussion
		3rd	Ch-02	Revision-2/ Previous yr Question Answer discussion
		4th	Ch-03	Revision-3/ Previous yr Question Answer discussion
		5th	Ch-04,05	Revision-4/ Previous yr Question Answer discussion
		6th	Ch-06,07	Revision-5/ Previous yr Question Answer discussion

Coverage of Chapters up to the internal assessment (2nd week of May): **1, 2 & 3.**

Learning Resources:

Sl. No.	Name of the Book	Author Name	Publisher
01	A.Kahate	Cryptography & Network Security	TMH
02	W. Stallings	Cryptography & Network Security Principles & Practices	Prentice Hall
03	Pachghare	Cryptography & Network Security	PHI