Department of Electronics and Communication Engineering		LP: **EC22072**
B.E/~~B.Tech/M.E/M.Tech~~	: **ECE** Regulation: **2022 (Autonomous)**	Rev. No: **00**
PG Specialisation	: **NOT APPLICABLE**	Date: **20/01/2025**
Sub. Code / Sub. Name	: **EC22072 CRYPTOGRAPHY AND NETWORK SECURITY**	
Unit	: **I**	

Unit Syllabus: SYMMETRIC AND ASYMMETRIC KEY CRYPTOGRAPHY (9)

Mathematics of Symmetric and Asymmetric key Cryptography: Overview - Symmetric Key Ciphers: Block Cipher Operation, RC4 - Asymmetric key Ciphers: Diffie-Hellman key exchange, SIDH, ElGamal cryptosystem, Elliptic curve cryptography

Objective: To understand various symmetric and asymmetric key cryptographic algorithms.

Session No.	Topics to be covered	Ref	Teaching Method
1.	Introduction to Cryptography	1,2,3,7	PPT/ICT
2.	Mathematics of Symmetric Key Cryptography	1,2,3	PPT/ICT
3.	Mathematics of Asymmetric Key Cryptography	1,2,3	PPT/ICT
4.	Block Cipher Operation	1,2,3	PPT/ICT
5.	Stream Cipher – RC4	1,2,3,7	PPT/ICT
6.	Diffie-Hellman key exchange	1,2,3	PPT/ICT
7.	SIDH	1,2,3	PPT/ICT
8.	ElGamal cryptosystem	1,2,3,7	PPT/ICT
9.	Elliptic Curve Cryptography	1,2,3	PPT/ICT
Content beyond the Syllabus: NIL			

* Session duration: 50 minutes

Sub. Code / Sub. Name : **EC22072 CRYPTOGRAPHY AND NETWORK SECURITY**
Unit : **II**

Unit Syllabus: AUTHENTICATION AND HASH FUNCTION **(9)**

Authentication requirements - Authentication functions - Message Authentication Codes - Hash Functions - Security of Hash Functions and MACs - Secure Hash Algorithm – HMAC - Digital Signatures - Authentication Protocols - Digital Signature Standard

Objective: To acquire fundamental knowledge on the concept of authentication and hash functions.

Session No.	Topics to be covered	Ref	Teaching Method
10.	Authentication requirements	1,2,3	PPT/ICT
11.	Authentication functions - Message Authentication Codes	1,2,3	PPT/ICT
12.	Authentication functions - Hash Functions	1,2,3	PPT/ICT
13.	Security of Hash Functions and MACs	1,2,3	PPT/ICT
14.	Secure Hash Algorithm	1,2,3,7	PPT/ICT
	FAT I	-	-
15.	HMAC	1,2,3	PPT/ICT
16.	Digital Signatures	1,2,3,7	PPT/ICT
17.	Authentication Protocols	1,2,3	PPT/ICT
18.	Digital Signature Standard	1,2,3	PPT/ICT
Content beyond the Syllabus: NIL			

* Session duration: 50 mins

Sub. Code / Sub. Name : **EC22072 CRYPTOGRAPHY AND NETWORK SECURITY**
Unit : **III**

Unit Syllabus: NETWORK SECURITY (9)

Authentication Applications: Kerberos - X.509 Authentication Service - Electronic Mail Security - PGP-S/MIME - IP Security: Architecture, Authentication Header - Web Security: Threats, Secure Electronic Transaction (SET).

Objective: To describe the principles of Electronic Mail Security and authentication services

Session No.	Topics to be covered	Ref	Teaching Method
19.	Authentication Applications - Kerberos	1,2,4,5,6	PPT/ICT
20.	X.509 Authentication Service	1,2,4,5	PPT/ICT
21.	Electronic Mail Security - PGP	1,2,4,5	PPT/ICT
22.	Electronic Mail Security - S/MIME	1,2,4,5,6	PPT/ICT
23.	IP Security - Architecture, Authentication Header	1,2,4,5,6	PPT/ICT
24.	IP Security – Encapsulating Security Payload	1,2,4,5,6	PPT/ICT
25.	Web Security - Threats	1,2,4,5,6	PPT/ICT
26.	Web Security – Secure Socket Layer (SSL)	1,2,4,5,6	PPT/ICT
27.	Web Security – Secure Electronic Transaction (SET)	1,2,4,5,6	PPT/ICT
Content beyond the Syllabus: NIL			

* Session duration: 50 mins

Sub. Code / Sub. Name : **EC22072 CRYPTOGRAPHY AND NETWORK SECURITY**
Unit : **IV**

Unit Syllabus: SYSTEM SECURITY **(9)**

Intrusion detection - Password Management - Viruses and related Threats - Virus Counter measures - Firewall Design Principles – Trusted Systems

Objective: To give an insight on various system level security concepts

Session No.	**Topics to be covered**	**Ref**	**Teaching Method**
28.	Intruders – Classes, techniques	1,2,4,5	PPT
29.	Intrusion detection	1,2,4,5	PPT
30.	Password Management	1,2,4,5	PPT
31.	Viruses and related Threats – Nature, types	1,2,4,5	PPT
32.	Viruses and related Threats – Macro, Email viruses	1,2,4,5	PPT
	FAT II	-	-
33.	Virus Counter measures	1,2,4,5	PPT
34.	Firewall Design Principles – Characteristics, types	1,2,4,5	PPT
35.	Firewall Design Principles - Configuration	1,2,4,5	PPT
36.	Trusted Systems – Honey Pots	1,2,4,5	PPT
Content beyond the Syllabus: Honey Pots			

* Session duration: 50 mins

Sub. Code / Sub. Name : **EC22072 CRYPTOGRAPHY AND NETWORK SECURITY**
Unit : **V**

Unit Syllabus: LIGHTWEIGHT AND POST-QUANTUM CRYPTOGRAPHY (9)
Lightweight Cryptography: Concepts, Algorithm – Post-Quantum Cryptography: Quantum Computing, Concepts, Algorithms

Objective: To expose the concepts of Lightweight and quantum cryptography

Session No.	**Topics to be covered**	**Ref**	**Teaching Method**
37.	Introduction to Lightweight Cryptography	1,2,3,5	PPT/ICT
38.	Lightweight Cryptography Concepts	1,2,3,5	PPT/ICT
39.	Lightweight Cryptographic Algorithm	1,2,3,5	PPT/ICT
40.	Introduction to Quantum Cryptography	1,2,3,5	PPT/ICT
41.	Post-Quantum Cryptography	1,2,3,5	PPT/ICT
42.	Quantum Computing	1,2,3,5	PPT/ICT
43.	Quantum Computing Concepts	1,2,3,5	PPT/ICT
44.	Quantum Computing Algorithms	1,2,3,5	PPT/ICT
45.	Practical Cryptography	1,2,3,5	PPT/ICT
	FAT III	-	-
Content beyond the Syllabus: Practical Cryptography			

* Session duration: 50 mins

Sub. Code / Sub. Name: **EC22072 CRYPTOGRAPHY AND NETWORK SECURITY**

References:

1. William Stallings, “Cryptography and Network Security: Principles and Practice”, 8th Edition, Prentice Hall of India, New Delhi, 2020.
2. William Stallings, "Cryptography and Network security: principles and practice", 4th Edition, Prentice Hall of India, New Delhi, 2005.
3. Parag K Lala, “Quantum Computing A Beginner’s Introduction”, McGraw- Hill, 2019.
4. Behrouz A. Forouzan Cryptography and Network security, McGraw- Hill, 2011.
5. Bruce Schneier and Neils Ferguson, “Practical Cryptography”, First Edition, Wiley Dreamtech India Pvt Ltd, 2003.
6. Man Young Rhee, “Internet Security: Cryptographic Principles”, “Algorithms and Protocols”, Wiley Publications, 2003.
7. https://onlinecourses.nptel.ac.in/noc19_cs28

	Prepared by	Approved by
Signature		
Name	Dr.T.J.Jeyaprabha / Ms.R.Kousalya	Dr.G.A.Sathish Kumar
Designation	Associate Professor / Assistant Professor	Professor & HOD - ECE
Date	20/01/2025	20/01/2025
Remarks*:		
Remarks*:		

* If the same lesson plan is followed in the subsequent semester/year it should be mentioned and signed by the Faculty and the HOD