

CSE11122	Introduction to Cyber Security	L	T	P	C
Version 1.0	Contact Hours 45	3	0	0	3
Pre-requisite/Exposure	Computer Network				
Co-requisite	NIL				

Course Objectives:

- To understand basics of Cyber Security.
- To be able to secure a message over insecure channel by various means.
- To learn about how to maintain the Confidentiality, Integrity and Availability of a data.
- To understand various protocols for cyber security to protect against the threats in the cyber space.

Course Outcomes:

On the completion of this course the student will be able to CO1. Define the basics of Cyber security and types of existing

malware. CO2. Understand and identify the cyber security breaches and cyber attacks.CO3. Explain the preventive measures for cyber fraud

CO4. Examine the basics concept of Social Network Security and Web Security.

CO5. Appraise the recent threats and attacks against the technical world and design some effective preventionscheme.

Course Description:

Effective network communication is an integral part of technical life. Cyber Security and Cryptography is a process ofsecuring the data communication, all the algorithms, messages etc. In this course you will learn the basics of cyber security and how to prevent and detect any sort of cyber attacks. The course begins with a detailed discussion of differenttypes of malware, cyber security breaches and cyber attacks. Throughout the course participants will be exposed to many exciting open problems in the field and work on fun (optional) programming projects. In the course cyber securitywe will cover more advanced security tasks such as zero- day vulnerability, privacy mechanisms, and other forms of defence against hackers.

Course Content:

Units	Lecture Hours
Unit-I: Cyber security fundamentals: Definition of cyber space, cyber security, importance of cyber security, hacker, related case studies Types of malware: Worm, virus, spyware, Trojan, related case studies	09
Unit-II	09

Units	Lecture Hours
Unit-09: Cyber security breaches: Phishing, identity theft, harassment, cyber stalking, related case studies Types of cyber attacks: Password attacks, Denial of service attacks, Passive attack, Penetration testing, related case studies	09
Unit-III: Prevention tips: Design a strong password, Two-step verification, Question validity of web-sites, related case studies Mobile protection: related case studies	09
Unit-IV: Social network security: Security measures like not revealing location, keeping birth-date hidden, having private profile, not linking accounts, related case study Prevention software: Firewalls, Virtual private network, Anti-virus & anti-spyware, Routine updates, related case study	09
Unit-V: Critical cyber threats: Critical cyber threats, cyber terrorism, cyber-warfare, cyber-espionage, Defense against hackers: Cryptography, digital forensics, intrusion detection, legal recourse, related course study	09

Examination Scheme:

Components	Mid Term	Class Assessment	End Term
Weightage (%)	20	30	50

Relationship between Course Outcomes (COs) and Program Outcomes (POs):

1 = Weakly Mapped

2 = Moderately Mapped 3 = Strongly Mapped

Course Code	Course Name	COs	PO 1	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
CSE11	Introduc	CO111	2	2	2	2	3	1	2	-	2	-	-	3	3	1	1
122	tion to	22.1															
	Cyber Security	CO111 22.2	1	3	3	1	3	3	3	-	3	-	-	1	3	1	1
		CO111	3	3	3	3	3	3	2	-	3	-	-	2	3	1	1
		22.3															
		CO111	3	3	2	2	1	3	3	-	1	-	-	3	2	1	1
		22.4															
		CO111	2	1	1	2	3	3	1	-	3	-	-	2	1	1	3
		22.5															
		CO111	2.	2.	2.	2.	2.	2.	2.	-	2.	-	-	2.2	2.4	1.0	1.4
		22	2	4	2	0	6	6	2		4						

