D. Syllabus Detailing and Learning objectives

Module	Chapter	Detailed Content	Syllabus Detailing	Learning Objectives
Module 1	**CH 1 Introduction** (Hours -03)	Introduction: Security Attacks, Security Goals, Computer Criminals, Methods of defense, Security Services, Security Mechanisms	**Purpose**: To make students understand importance of security goals. Explain the different vulnerabilities in computing system. Describe Method of defense. Explain security mechanism. **Scope –** **1. Academic Aspects-** Compare the role and application of various security goals. **2. Technology Aspect-** Understand Agile methodology. **3. Application Aspect-** Typical applications for each model **Students Evaluation** – 1. Theory Questions to be asked on Security attacks & Goals 2. Lab experiments: case study can be done on all types of attacks & control system. 3. Corresponding viva questions can be asked on attacks & security mechanism.	1. To Describe the security attacks for computing system. **(R)** 2. To Describe the various process models- Incremental and Evolutionary models **(R)** 3.To Distinguish between the process models **(U)**
Module 2	**CH 2 Basics of Cryptography:** (Hours -06)	Basics of Cryptography: Symmetric Cipher Model, Substitution Techniques, Transportation Techniques, Other Cipher Properties- Confusion, Diffusion, Block and Stream Ciphers.	**Purpose** – To make students learn the importance of cryptographic algorithm. Study the cryptanalysis technique. Learn about the block cipher & stream cipher. **Scope –** **1. Academic Aspects-** Identify the various attacks in the system. Decide the best suitable algorithm to avoid the attacks. Plan for the control of attacks. **2. Technology Aspect-**Discuss the possibilities of cracking the code in all the algorithms. Comparison of block cipher & stream cipher.	1. To identify the causes of attack & provide security while transmitting the data through different algorithms. **(AN)** 2. To Estimate the way for cryptanalysis if student knows the cipher text. **(E)**

			3. Application Aspect- to help the developer to enhance the algorithms to protect the system.	3. Illustrate the working of all the algorithms.**(A)** 4. To distinguish between block cipher & stream cipher (U) 5. To design a block cipher algorithm with different key size & permutation methods. 6. Explain DES algorithm in detail. (U)
			Students Evaluation 1. Questions on Effort/Cost estimation and its solution based on the type of attacks. 2. Lab experiment based on implementation of algorithms. 3. Viva questions on cryptographic technique.	
	Chapter 3 :Secret Key Cryptography	Data Encryption Standard(DES), Strength of DES, Block Cipher Design Principles and Modes of Operations, Triple DES, International Data Encryption algorithm, Blowfish, CAST-128.	**Purpose** – To make students learn the importance of block cipher. Study the design & principles of block cipher. Learn about different types of block cipher its advantages & disadvantages	
			Scope – **1. Academic Aspects-** Identify need of block cipher and key size. Decide the best suitable algorithm to avoid the attacks & improve efficiency **2. Technology Aspect-**Discuss the possibilities of cracking the code in all the algorithms. Compare all the block ciphers based on 32 or 64 bit microprocessor and key size. **3. Application Aspect-** To help the developer to enhance the algorithms to protect the system & improve efficiency of the algorithm as well as utilization in all the applications.	
			Students Evaluation 1. Questions on DES & types of DES 2. Lab experiment based on implementation of algorithms. 3. Viva questions on block ciphers & different key size & its usage	
	Chapter 4: Public Key Cryptography	Principles of Public Key Cryptosystems, RSA Algorithm, Diffie-Hellman Key Exchange	**Purpose** – To make students understand the public key cryptosystem and types of keys used in the algorithm. Learn public key generation and how to use it in the system to make it secure.	1. To distinguish between symmetric key & asymmetric key cryptography. (U) 2. Explain RSA algorithm with example? (A)

Module 3			**Scope –** **1. Academic Aspects-** Identify the weakness in the symmetric key cryptographic algorithm and overcome by implementing asymmetric key cryptographic algorithm. **2. Technology Aspect-** Decide the key size to make the system secure. Product of two keys should be 309 decimal digit. **3. Application Aspect-** To help the developer to keep the public key open to all and secure the private key.	3. Describe man in the middle attack in Diffie Hellman. (U)
			Students Evaluation 1. Questions on RSA & Diffie Hellaman algorithm 2. Lab experiment based on implementation of algorithms. 3. Viva questions on public key cryptography & how it is different from symmetric key cryptography.	
	Chapter 5: Cryptographic Hash Functions	Applications of Cryptographic Hash Functions, Secure Hash Algorithm, Message Authentication Codes – Message Authentication Requirements and Functions, HMAC, Digital signatures, Digital Signature Schemes,	**Purpose** – To make students learn the importance of hashing in cryptography. How hashing can provide security to the system. Learn use of private key in the Digital Signature. Provide authentication & authorization in the system.	4. Explain the Authentication protocols and it's applications. **(U)** 4. Distinguish between MD5 & SHA. **(U)** 5. Apply the protocols to enhance the security in public key cryptography. **(A)**
			Scope – **1. Academic Aspects-** Identify system which requires authentication and how to provide security using hashing & digital signature. **2. Technology Aspect-**Discuss the different hashing algorithm finds out advantages and efficiency of each algorithm. **3. Application Aspect-** To help the developer to enhance the algorithms by providing hashed key which will be difficult to break by intruder and improve efficiency of algorithm.	

		Authentication Protocols, Digital Signature Standards.	**Students Evaluation** 1. Questions on HMAC & Digital Signature 2. Lab experiment based on providing digital signature 3. Viva questions on hashing techniques and authentication protocols	
Module 4	**Authentication Applications (Hours-06)**	Kerberos, Authentication Mechanisms, E-Mail security, PGP, S/MIME	**Purpose –** To make the student understand the importance of Authentication as a security mechanism & also to understand it's applications. **Scope –** **1. Academic Aspects-** To learn the role of Authentication Mechanisms in networked system and apply in areas like E-Mail security, etc. **2. Technology Aspect-** To make use of Authentication methods in the areas like Email security, etc. **3. Application Aspect-** To apply the authentication methods in critical infrastructure areas. **Student Evaluation -** 1.Questions based on Kerberos Authentication Protocol. 2. Mini project: Develop a mechanism to secure E-Mails. 3. GATE questions based on Kerberos Authentication Protocol, PGP, SMIME.	1. Describe the importance of Authentication mechanisms, Public Key Infrastructure and Digital Certificates **(R)** as an effective security mechanism. **(U)** 2. Compare the security levels based on the various protocols applied to critical infrastructure areas. **(U)** 3. Explain the Authentication protocols and it's applications in infrastructure areas. **(U)** 4. Distinguish between Authentication and Authorization. **(U)** 5. Apply the protocols to enhance the security in E-Mails. **(A)** 6.Develop the methodology to make secure the communication messages in transit using Public Key Infrastructure and Digital Certificates. **(C)**
Module 5	**Chapter 7** **Program**	Secure programs, Nonmalicious Program Errors, Malicious Software –	**Purpose –** This chapter explains the need of Security in Computing Systems. Understand the vulnerabilities in various parts of the computer system (Programs, Operating System, Databases, Network)	1. Describe the various attacks under Program, Operating System, Databases and Network Security. **(U)**

	Security, Operating System Security, Database Security, IDS and Firewalls (Hours - 08)	Types, Viruses, Virus Countermeasures, Worms , Targeted Malicious Code, Controls against Program Threats. Memory and Address protection, File Protection Mechanism, User Authentication. Security Requirement, Reliability and Integrity, Sensitive data, Inference, Multilevel Databases Intruders, Intrusion Detection, Password Management, Firewalls-Characteristics, Types of Firewalls, Placement of Firewalls, Firewall Configuration, Trusted systems.	**Scope –** **1. Academic Aspects-** Understand the basic concepts in learning the vulnerabilities and threats (like effects of Viruses, Malicious Codes) in different parts of the computer system with critical data. **2. Technology Aspect-** Design of anti-viruses, defense mechanisms, etc. to protect against threats and attacks. **3. Application Aspect-** To apply the defense mechanisms in each part of the computer systems. **Student Evaluation –** 1. Theory and viva questions on Viruses, Malicious Codes, threats and attacks under Programs, Operating Systems, Databases and Networked Computing Systems. 2. Mini project: Configure a Firewall using IP tables or create an IDS. 3. GATE questions based on Firewall, IDS, Viruses, Malicious Codes, Buffer Overflow Attacks.	2. Apply the methods of defense for the various parts of the computing system**. (U)** 3. Design the configuration rules for implementing the Firewalls and IDS's. **(C)** 4. Discuss the variation in threats and attacks under different parts of the computing systems to build an effective defense mechanism. **(A)** 5. Explain the importance of protection of Sensitive Data and how it can be protected against the threats and attacks. **(U)** 6. List the different types of attacks in Programs, Operating System, Databases and Networked Systems. **(U)**
Module 6	**Chapter 8 IP Security**	Overview	**Purpose –** Discuss the importance of IP Security, Tunnel Mode	. Describe the various vulnerabilities under TCP/IP Model**. (U)**

	(Hours - 06)	Payload Transport Layer Security DoS, DDoS, Session Hijacking and Spoofing, Software Vulnerabilities- Phishing, Buffer Overflow, Format String Attacks, SQL Injection	Encapsulation of data, Internet Key Exchange, Secure Socket Layer, Web Security, and Transport Layer Security as Security Mechanisms and understand in depth the TCP/IP vulnerabilities. **Scope –** **1. Academic Aspects-** Explain the basics of IP Security. **2. Technology Aspect-** Study of Non-Cryptographic Protocol Vulnerabilities. **3. Application Aspect-** Apply the various methods of defense to reduce the risk levels of TCP/IP attacks **Student Evaluation –** 1. Theory and viva questions on Authentication Header. 2. Lab experiments based on SSL. 3. GATE questions on IP Security, DOS attacks, TCP/IP attacks.	2. Analyze the level of risk involved in web based applications**. (A)** 3. Explain the importance of Web Security. **(U)** 4. List attacks under the TCP/IP. Cite the scenarios in which the attacks have **(U)** 5. Describe IP Security. **(U)** 6. Specify the need of Web Security. (C).