INSTITUTE OF AERONAUTICAL ENGINEERING
(Autonomous)
Dundigal, Hyderabad - 500 043

INFORMATION TECHNOLOGY
DEFINITION AND TERMINOLGY

Course Title	**CRYPTOGRAPHY AND NETWORK SECURITY**				
Course Code	AITC11				
Program	B.Tech				
Semester	V	IT			
Course Type	Core				
Regulation	UG-20				
Course Structure	Theory			Practical	
	Lecture	Tutorials	Credits	Laboratory	Credits
	3	1	4	-	-
Course Coordinator	Dr. PL Srinivasa Murthy				

COURSE OBJECTIVES:
The students will try to learn:

I	The security standards and practices. The scope and essentiality of threats, attacks to computers and networks associated to them.
II	The symmetric and asymmetric key generation techniques used for providing message authentication, confidentiality and Integrity.
III	The use cases on cryptography and security systems for server and client systems such as web, email and firewalls..

COURSE OUTCOMES:
After successful completion of the course, students should be able to:

CO 1	**Outline** model for network security and cryptographic algorithms to prevent attacks on computer and computer security.	Understand
CO 2	**Demonstrate** symmetric and asymmetric key ciphers for messaging end to end encryption used in different types of cryptographic algorithms.	Understand
CO 3	**Make use of** tools and protocols used in message authentication and hashing functions for every day computing to remain secure.	Apply
CO 4	**Choose** appropriate architecture and protocols used in email and IP security to protect against attackers and intruders.	Apply

CO 5	**Select** firewalls to provide web security as case study in cryptography and network security	Apply
CO 6	**Utilize** cryptographic and security algorithms to enhance defence against cyber attacks and to improve organization working culture.	Apply

DEFINITION AND TERMINOLOGY:

S.No	DEFINITION	CO's
	MODULE I	
	ATTACKS ON COMPUTERS AND COMPUTER SECURITY	
1	**What is security attack?**	CO 1
	Any action that compromises the security of information owned by an organization.	
2	**Explain security mechanism?**	CO 1
	A process that is designed to detect or prevent or recover from a security attack.	
3	**Define security service?**	CO 1
	A processing or communication service that enhances the security of the data processing systems and the information transfers of an organization	
4	**What is peer entity authentication?**	CO 1
	Provides for the corroboration of the identity of a peer entity in an association. It is provided for use at the establishment of a connection	
5	**Explain threat?**	CO 1
	A potential for violation of security, which exists when there is a circumstance or event that could breach security and cause harm.	
6	**Define access control?**	CO 1
	Access control is the ability to limit and control the access to host systems and applications via communications links.	
7	**Explain non repudiation?**	CO 1
	Non repudiation prevents either sender or receiver from denying a transmitted message. Thus, when a message is sent, the receiver can prove that the alleged sender in fact sent the message. Similarly, when a message is received, the sender can prove that the alleged receiver in fact received the message.	
8	**Define authentication exchange?**	CO 1
	A mechanism intended to ensure the identity of an entity by means of information exchange.	
9	**What is traffic padding?**	CO 1
	The insertion of bits into gaps in a data stream to frustrate traffic analysis attempts. .	

10	**Explain routing control?**	CO 1
	Enables selection of particular physically secure routes for certain data and allows routing changes, especially when a breach of security is suspected	
11	**Define notarization?**	CO 1
	The use of a trusted third party to assure certain properties of a data exchange.	
12	**What is security label?**	CO 1
	The marking bound to a resource that names or designates the security attributes of that resource	
13	**Define security audit trail?**	CO 1
	Data collected and potentially used to facilitate a security audit, which is an independent review and examination of system records and activities	
14	**Explain security recovery?**	CO 1
	Deals with requests from mechanisms, such as event handling and management functions and takes recovery actions.	
15	**What is meant by information access threat?**	CO 1
	Intercept or modify data on behalf of users who should not have access to that data	
16	**Define service threat?**	CO 1
	Exploit service flaws in computers to inhibit use by legitimate users.	
17	**What is plaintext?**	CO 1
	An original message is known as the plaintext.	
18	**What is enciphering?**	CO 1
	The process of converting from plaintext to cipher text is known as enciphering or encryption	
19	**Define cryptanalysis?**	CO 1
	Techniques used for deciphering a message without any knowledge of the enciphering details fall into the area of cryptanalysis	
	MODULE II	
	SYMMETRIC KEY CIPHERS	
1	**Explain block cipher?**	CO 2
	A block cipher is an encryption/decryption scheme in which a block of plaintext is treated as a whole and used to produce a cipher text block of equal length	
2	**Define stream cipher?**	CO 2
	A stream cipher is one that encrypts a digital data stream one bit or one byte at a time.	
3	**What is meant by diffusion?**	CO 2
	The statistical structure of the plaintext is dissipated into long-range statistics of the cipher text.	

4	**Explain confusion?** The relationship between the statistics of the cipher text and the value of the encryption key as complex as possible	CO 2
5	**What is avalanche effect?** A desirable property of any encryption algorithm is that a small change in either the plaintext or the key should produce a significant change in the cipher text	CO 2
6	**Explain timing attack?** A timing attack is one in which information about the key or the plaintext is obtained by observing how long it takes a given implementation to perform decryptions on various cipher text	CO 2
7	**Define differential cryptanalysis?** Differential cryptanalysis is to observe the behavior of pairs of text blocks evolving along each round of the cipher, instead of observing the evolution of a single text block	CO 2
8	**What is key agility?** Key agility refers to the ability to change keys quickly and with a minimum of resources	CO 2
9	**What is add round key?** A simple bitwise XOR of the current block with a portion of the expanded key.	CO 2
10	**Define nibble substitution?** A permutation of all possible 4-bit values which is used by AES.	CO 2
11	**Explain Electronic codebook?** Each block of 64 plaintext bits is encoded independently using the same key.	CO 2
12	**Define Cipher Block Chaining?** The input to the encryption algorithm is the XOR of the next 64 bits of plaintext and the preceding 64 bits of cipher text.	CO 2
13	**Explain Cipher Feedback?** Input is processed j bits at a time. Preceding cipher text is used as input to the encryption algorithm to produce pseudorandom output, which is XORed with plaintext to produce next unit of cipher text.	CO 2
14	**Define counter mode?** Each block of plaintext is XORed with an encrypted counter. The counter is incremented for each subsequent block.	CO 2
15	**Explain key distribution?** Key distribution is the function that delivers a key to two parties who wish to exchange secure encrypted data	CO 2

MODULE III		
MESSAGE AUTHENTICATION ALGORITHM AND HASH FUNCTIONS		
1	**What is meant message authentication?**	CO 3
	Message authentication is a mechanism or service used to verify the integrity of a message. Message authentication assures that data received are exactly as sent by and that the purported identity of the sender is valid	
2	**Define masquerade?**	CO 3
	Insertion of messages into the network from a fraudulent source. This includes the creation of messages by an opponent that are purported to come from an authorized entity.	
3	**What is source repudiation?**	CO 3
	Denial of transmission of message by source.	
4	**What is sequence modification?**	CO 3
	Any modification to a sequence of messages between parties, including insertion, deletion, and reordering.	
5	**Define message authentication code?**	CO 3
	A function of the message and a secret key that produces a fixed-length value that serves as the authenticator	
6	**Explain hash code?**	CO 3
	A function that maps a message of any length into a fixed-length hash value, which serves as the authenticator	
7	**Define X.509.authentication?**	CO 3
	X.509 defines the format for public-key certificates. This format is widely used in a variety of applications.	
8	**Explain Kerberos?**	CO 3
	Kerberos makes use of a trusted third-part authentication service that enables clients and servers to establish authenticated communication.	
9	**Explain public key infrastructure?**	CO 3
	A public key infrastructure (PKI) is defined as the set of hardware, software, people, policies, and procedures needed to create, manage, store, distribute, and revoke digital certificates based on asymmetric cryptography.	
10	**Define subkey?**	CO 3
	The client's choice for an encryption key to be used to protect this specific application session	
11	**What is authentication identifier?**	CO 3
	Identifies the public key to be used to verify the signature on this certificate.	

12	**Define end entity in certification authority?**	CO 3
	A generic term used to denote end users, devices or any other entity that can be identified in the subject field of a public key certificate.	
13	**Define repository in certification authority?**	CO 3
	A generic term used to denote any method for storing certificates and CRLs so that they can be retrieved by End Entities.	
14	**Explain cross certification**	CO 3
	A cross-certificate is a certificate issued by one CA to another CA that contains a CA signature key used for issuing certificates.	
15	**What is meant digital signature?**	CO 3
	The signature must use some information unique to the sender, to prevent both forgery and denial.	
MODULE IV		
E-MAIL SECURITY		
1	**What is meant enveloped data?**	CO 4
	This consists of encrypted content of any type and encrypted-content encryption keys for one or more recipients.	
2	**Explain signed data.**	CO 4
	A digital signature is formed by taking the message digest of the content to be signed and then encrypting that with the private key of the signer	
3	**What is the full form of MIME?**	CO 4
	Multipurpose Internet Mail Extensions	
4	**Explain Encapsulating Security Payload?**	CO 4
	Covers the packet format and general issues related to the use of the ESP for packet encryption	
5	**What is meant security association?**	CO 4
	A key concept that appears in both the authentication and confidentiality mechanisms for IP is the security association.	
6	**Explain the purpose of security parameter index?**	CO 4
	The security parameter index is carried in AH and ESP headers to enable the receiving system to select the SA under which a received packet will be processed.	
7	**What is transport mode ESP?**	CO 6
	Authentication and encryption apply to the IP payload delivered to the host, but the IP header is not protected.	
8	**What is tunnel mode ESP?**	CO 4
	Authentication applies to the entire IP packet delivered to the outer IP destination address and authentication is performed at that destination.	

9	**Define transport adjacency?**	CO 4
	Refers to applying more than one security protocol to the same IP packet, without invoking tunneling	
10	**Explain Oakley Key Determination Protocol?**	CO 4
	Oakley is a key exchange protocol based on the Diffie-Hellman algorithm but providing added security	
11	**Explain ISAKMP?**	CO 4
	ISAKMP provides a framework for Internet key management and provides the specific protocol support, including formats, for negotiation of security attributes.	
12	**What is the full form of ISAKMP?**	CO 4
	Internet Security Association and Key Management Protocol.	
13	**What is meant time to alive?**	CO 4
	Specifies how long, in seconds, a packet is allowed to remain in the internet.	
14	**Define fragmentation?**	CO 4
	Packets from one network may have to be broken into smaller pieces to be transmitted on another network	
15	**What is the full form of PGP?**	CO 4
	Pretty Good Privacy	
MODULE V		
CONNECT TO AN EXTERNAL API		
1	**Explain masquerader?**	CO 5
	An individual who is not authorized to use the computer and who penetrates a system's access controls to exploit a legitimate user's account	
2	**Define misfeasor?**	CO 5
	A legitimate user who accesses data, programs, or resources for which such access is not authorized, or who is authorized for such access but misuses his or her privileges.	
3	**What is meant statistical anomaly detection?**	CO 6
	Then statistical tests are applied to observed behavior to determine with a high level of confidence whether that behavior is not legitimate user behavior	
4	**Explain Clandestine user**	CO 5
	An individual who seizes supervisory control of the system and uses this control to evade auditing and access controls or to suppress audit collection	
5	**Define threshold detection?**	CO 5
	This approach involves defining thresholds, independent of user, for the frequency of occurrence of various events.	

6	**What is rule based detection?**	CO 6
	Involves an attempt to define a set of rules that can be used to decide that a given behavior is that of an intruder.	
7	**Define virus?**	CO 5
	Attaches itself to a program and propagates copies of itself to other programs	
8	**Explain worm?**	CO 5
	Program that propagates copies of itself to other computers	
9	**What is meant dormant phase in virus detection?**	CO 5
	The virus will eventually be activated by some event, such as a date, the presence of another program or file, or the capacity of the disk exceeding some limit.	
10	**Define propagation phase in virus detection?**	CO 6
	The virus places an identical copy of itself into other programs or into certain system areas on the disk.	
11	**Explain triggering phase in virus detection?**	CO 6
	The virus is activated to perform the function for which it was intended.	
12	**What is parasitic virus?**	CO6
	A parasitic virus attaches itself to executable files and replicates, when the infected program is executed, by finding other executable files to infect.	
13	**Define firewall?**	CO 5
	A firewall forms a barrier through which the traffic going in each direction must pass. A firewall security policy dictates which traffic is authorized to pass in each direction.	
14	**Explain packet filtering router?**	CO 5
	A packet-filtering router applies a set of rules to each incoming and outgoing IP packet and then forwards or discards the packet	
15	**What is the responsibility of Internet Engineering Task Force (IETF)?**	CO 5
	The protocol engineering and development arm of the Internet	

Course Coordinator: **HOD IT**
Dr. PL Srinivasa Murthy