INSTITUTE OF AERONAUTICAL ENGINEERING

(Autonomous)
Dundigal, Hyderabad - 500 043

COMPUTER SCIENCE AND ENGINEERING

DEFINITIONS AND TERMINOLOGY QUESTION BANK

Course Name	:	**INFORMATION SECURITY**
Course Code	:	**ACS013**
Program	:	**B.Tech**
Semester	:	**VIII**
Branch	:	**Computer Science and Engineering**
Section	:	**A,B,C,D**
Course Faculty	:	**Ms B Geetavani, Assistant Professor** **Ms B Anupama, Assistant Professor** **Ms B Swathi, Assistant Professor** **Ms P Navya, Assistant Professor**

OBJECTIVES:

I	Help students to consider in depth the terminology and nomenclature used in the syllabus.
II	Focus on the meaning of new words / terminology/nomenclature.

DEFINITIONS AND TERMINOLOGYQUESTION BANK

S.No	QUESTION	ANSWER	Blooms Taxonomy Level	CLO	CO	CLO Code
		UNIT-I				
1	What is security attack?	Any action that compromises the security of information owned by an organization.	Understand	CLO1	CO1	ACS013.01
2	Explain security mechanism.	A process that is designed to detect or prevent or recover from a security attack.	Remember	CLO1	CO1	ACS013.01
3	Define security service.	A processing or communication service that enhances the security of the data processing systems and the information transfers of an organization.	Understand	CLO1	CO1	ACS013.01
4	What is peer entity authentication?	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.	Remember	CLO1	CO1	ACS013.01
5	Explain threat.	A potential for violation of security, which exists when there is a circumstance or event that could breach security and cause harm.	Remember	CLO1	CO1	ACS013.01
6	Define access control.	Access control is the ability to limit and control the access to host systems and applications via communications links.	Understand	CLO1	CO1	ACS013.01
7	Explain non repudiation.	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.	Remember	CLO1	CO1	ACS013.01

S.No	QUESTION	ANSWER	Blooms Taxonomy Level	CLO	CO	CLO Code
8	Define authentication exchange.	A mechanism intended to ensure the identity of an entity by means of information exchange.	Remember	CLO1	CO1	ACS013.01
9	What is traffic padding?	The insertion of bits into gaps in a data stream to frustrate traffic analysis attempts.	Understand	CLO1	CO1	ACS013.01
10	Explain routing control.	Enables selection of particular physically secure routes for certain data and allows routing changes, especially when a breach of security is suspected.	Remember	CLO1	CO1	ACS013.01
11	Define notarization.	The use of a trusted third party to assure certain properties of a data exchange.	Remember	CLO1	CO1	ACS013.01
12	What is security label?	The marking bound to a resource that names or designates the security attributes of that resource.	Understand	CLO1	CO1	ACS013.01
13	Define security audit trail.	Data collected and potentially used to facilitate a security audit, which is an independent review and examination of system records and activities.	Remember	CLO1	CO1	ACS013.01
14	Explain security recovery.	Deals with requests from mechanisms, such as event handling and management functions and takes recovery actions.	Remember	CLO1	CO1	ACS013.01
15	What is meant information access threat?	Intercept or modify data on behalf of users who should not have access to that data	Understand	CLO2	CO1	ACS013.02
16	Define service threat.	Exploit service flaws in computers to inhibit use by legitimate users.	Remember	CLO2	CO1	ACS013.02
17	What is plaintext?	An original message is known as the plaintext.	Understand	CLO5	CO1	ACS013.05
18	What is enciphering?	The process of converting from plaintext to ciphertext is known as enciphering or encryption.	Understand	CLO5	CO1	ACS013.05
19	Define cryptanalysis.	Techniques used for deciphering a message without any knowledge of the enciphering details fall into the area of cryptanalysis.	Remember	CLO5	CO1	ACS013.05
20	Explain secret key.	The secret key is also input to the encryption algorithm. The key is a value independent of the plaintext and of the algorithm. The algorithm will produce a different output depending on the specific key being used at the time. The exact substitutions and transformations performed by the algorithm depend on the key.	Remember	CLO5	CO1	ACS013.05
		UNIT-II				
1	Explain block cipher.	A block cipher is an encryption/decryption scheme in which a block of plaintext is treated as a whole and used to produce a ciphertext block of equal length.	Remember	CLO7	CO2	ACS013.07
2	Define stream cipher.	A stream cipher is one that encrypts a digital data stream one bit or one byte at a time.	Remember	CLO8	CO2	ACS013.08
3	What is meant by diffusion?	The statistical structure of the plaintext is dissipated into long-range statistics of the ciphertext.	Understand	CLO6	CO2	ACS013.06
4	Explain confusion.	The relationship between the statistics of the ciphertext and the value of the encryption key as complex as possible	Remember	CLO6	CO2	ACS013.06
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 ciphertext.	Understand	CLO6	CO2	ACS013.06

S.No	QUESTION	ANSWER	Blooms Taxonomy Level	CLO	CO	CLO Code
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 ciphertext	Remember	CLO6	CO2	ACS013.06
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.	Remember	CLO6	CO2	ACS013.06
8	What is key agility?	Key agility refers to the ability to change keys quickly and with a minimum of resources.	Understand	CLO9	CO2	ACS013.09
9	What is add round key?	A simple bitwise XOR of the current block with a portion of the expanded key.	Understand	CLO6	CO2	ACS013.06
10	Define nibble substitution.	A permutation of all possible 4-bit values which is used by AES.	Remember	CLO6	CO2	ACS013.06
11	Explain Electronic codebook.	Each block of 64 plaintext bits is encoded independently using the same key.	Remember	CLO8	CO2	ACS013.08
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 ciphertext.	Remember	CLO8	CO2	ACS013.08
13	Explain Cipher Feedback.	Input is processed j bits at a time. Preceding ciphertext is used as input to the encryption algorithm to produce pseudorandom output, which is XORed with plaintext to produce next unit of ciphertext.	Remember	CLO8	CO2	ACS013.08
14	Define counter mode.	Each block of plaintext is XORed with an encrypted counter. The counter is incremented for each subsequent block.	Remember	CLO8	CO2	ACS013.08
15	Explain key distribution.	Key distribution is the function that delivers a key to two parties who wish to exchange secure encrypted data	Remember	CLO10	CO2	ACS013.10
		UNIT-III				
1	What is meant message authentication?	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.	Understand	CLO11	CO3	ACS013.11
2	Define masquerade?	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.	Remember	CLO11	CO3	ACS013.11
3	What is source repudiation?	Denial of transmission of message by source.	Understand	CLO11	CO3	ACS013.11
4	What is sequence modification?	Any modification to a sequence of messages between parties, including insertion, deletion, and reordering.	Understand	CLO11	CO3	ACS013.11
5	Define message authentication code.	A function of the message and a secret key that produces a fixed-length value that serves as the authenticator	Remember	CLO11	CO3	ACS013.11
6	Explain hash code?	A function that maps a message of any length into a fixed-length hash value, which serves as the authenticator	Remember	CLO13	CO3	ACS013.13
7	Define X.509.	X.509 defines the format for public-key certificates. This format is widely used in a variety of applications.	Understand	CLO14	CO3	ACS013.14

S.No	QUESTION	ANSWER	Blooms Taxonomy Level	CLO	CO	CLO Code
8	Explain Kerberos.	Kerberos makes use of a trusted third-part authentication service that enables clients and servers to establish authenticated communication.	Remember	CLO14	CO3	ACS013.14
9	Explain public key infrastructure.	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.	Understand	CLO14	CO3	ACS013.14
10	Define subkey.	The client's choice for an encryption key to be used to protect this specific application session.	Remember	CLO12	CO3	ACS013.12
11	What is authentication identifier?	Identifies the public key to be used to verify the signature on this certificate.	Understand	CLO11	CO3	ACS013.11
12	Define end entity in certification authority.	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.	Remember	CLO14	CO3	ACS013.14
13	Define repository in certification authority.	A generic term used to denote any method for storing certificates and CRLs so that they can be retrieved by End Entities.	Remember	CLO14	CO3	ACS013.14
14	Explain cross certification.	A cross-certificate is a certificate issued by one CA to another CA that contains a CA signature key used for issuing certificates.	Remember	CLO14	CO3	ACS013.14
15	What is meant digital signature?	The signature must use some information unique to the sender, to prevent both forgery and denial.	Remember	CLO14	CO3	ACS013.14
	UNIT-IV					
1	What is meant enveloped data?	This consists of encrypted content of any type and encrypted-content encryption keys for one or more recipients.	Understand	CLO15	CO4	**ACS013.15**
2	Explain signed data.	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.	Remember	CLO15	CO4	ACS013.15
3	What is the full form of MIME?	Multipurpose Internet Mail Extensions	Understand	CLO15	CO4	ACS013.15
4	Explain Encapsulating Security Payload.	Covers the packet format and general issues related to the use of the ESP for packet encryption.	Understand	CLO16	CO4	ACS013.16
5	What is meant security association.	A key concept that appears in both the authentication and confidentiality mechanisms for IP is the security association.	Remember	CLO16	CO4	ACS013.16
6	Explain the purpose of security parameter index.	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.	Remember	CLO16	CO4	ACS013.16
7	What is transport mode ESP?	Authentication and encryption apply to the IP payload delivered to the host, but the IP header is not protected.	Understand	CLO16	CO4	ACS013.16
8	What is tunnel mode ESP?	Authentication applies to the entire IP packet delivered to the outer IP destination address and authentication is performed at that destination.	Understand	CLO16	CO4	ACS013.16

S.No	QUESTION	ANSWER	Blooms Taxonomy Level	CLO	CO	CLO Code
9	Define transport adjacency.	Refers to applying more than one security protocol to the same IP packet, without invoking tunneling.	Remember	CLO16	CO4	ACS013.16
10	Explain Oakley Key Determination Protocol.	Oakley is a key exchange protocol based on the Diffie-Hellman algorithm but providing added security.	Remember	CLO16	CO4	ACS013.16
11	Explain ISAKMP.	ISAKMP provides a framework for Internet key management and provides the specific protocol support, including formats, for negotiation of security attributes.	Remember	CLO16	CO4	ACS013.16
12	What is the full form of ISAKMP?	Internet Security Association and Key Management Protocol.	Understand	CLO16	CO4	ACS013.16
13	What is meant time to alive.	Specifies how long, in seconds, a packet is allowed to remain in the internet.	Understand	CLO16	CO4	ACS013.16
14	Define fragmentation.	Packets from one network may have to be broken into smaller pieces to be transmitted on another network.	Remember	CLO16	CO4	ACS013.16
15	What is the full form of PGP?	Pretty Good Privacy.	Remember	CLO16	CO4	ACS013.16
		UNIT-V				
1	Explain masquerader.	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	Remember	CLO17	CO5	ACS013.17
2	Define misfeasor.	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.	Remember	CLO17	CO5	ACS013.17
3	What is meant statistical anomaly detection?	Then statistical tests are applied to observed behavior to determine with a high level of confidence whether that behavior is not legitimate user behavior.	Understand	CLO18	CO5	ACS013.18
4	Explain Clandestine user.	An individual who seizes supervisory control of the system and uses this control to evade auditing and access controls or to suppress audit collection	Remember	CLO18	CO5	ACS013.18
5	Define threshold detection.	This approach involves defining thresholds, independent of user, for the frequency of occurrence of various events.	Remember	CLO18	CO5	ACS013.18
6	What is rule based detection?	Involves an attempt to define a set of rules that can be used to decide that a given behavior is that of an intruder.	Understand	CLO18	CO5	ACS013.18
7	Define virus.	Attaches itself to a program and propagates copies of itself to other programs.	Remember	CLO19	CO5	ACS013.19
8	Explain worm.	Program that propagates copies of itself to other computers.	Remember	CLO19	CO5	ACS013.19
9	What is meant dormant phase in virus detection?	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.	Understand	CLO19	CO5	ACS013.19
10	Define propagation phase in virus detection.	The virus places an identical copy of itself into other programs or into certain system areas on the disk.	Remember	CLO19	CO5	ACS013.19

S.No	QUESTION	ANSWER	Blooms Taxonomy Level	CLO	CO	CLO Code
11	Explain triggering phase in virus detection.	The virus is activated to perform the function for which it was intended.	Remember	CLO19	CO5	ACS013.19
12	What is parasitic virus?	A parasitic virus attaches itself to executable files and replicates, when the infected program is executed, by finding other executable files to infect.	Understand	CLO19	CO5	ACS013.19
13	Define firewall.	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.	Remember	CLO20	CO5	ACS013.20
14	Explain packet filtering router.	A packet-filtering router applies a set of rules to each incoming and outgoing IP packet and then forwards or discards the packet.	Remember	CLO20	CO5	ACS013.20
15	What is the responsibility of Internet Engineering Task Force (IETF)?	The protocol engineering and development arm of the Internet	Understand	CLO17	CO5	ACS013.17

Signature of the Faculty **Signature of HOD**