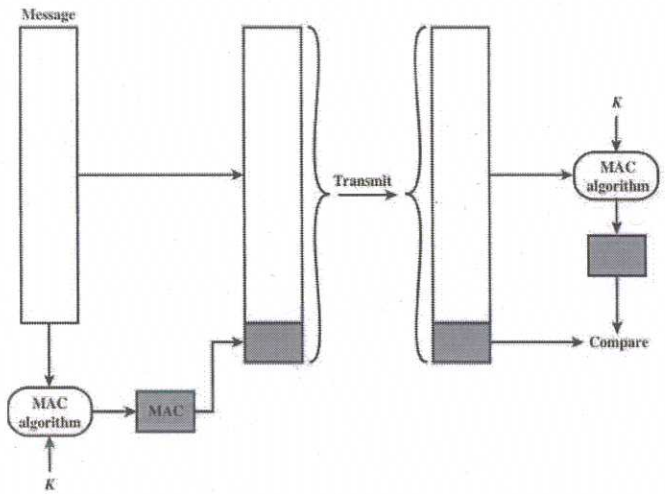
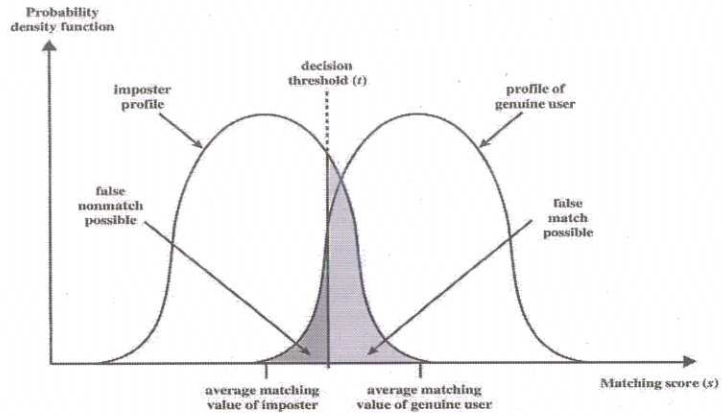
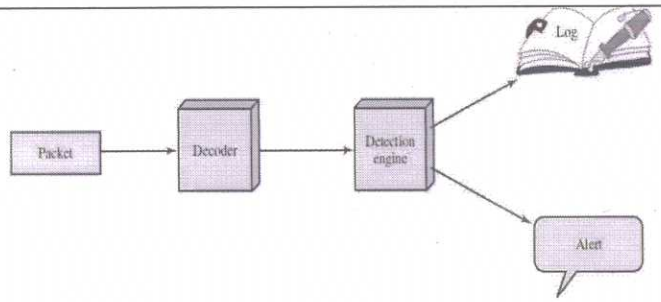
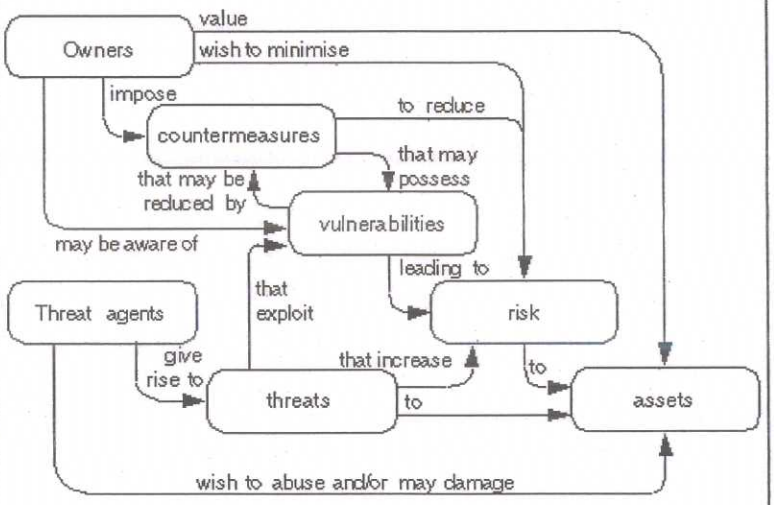
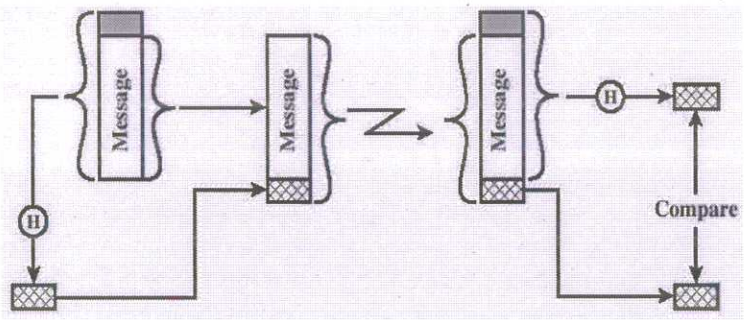
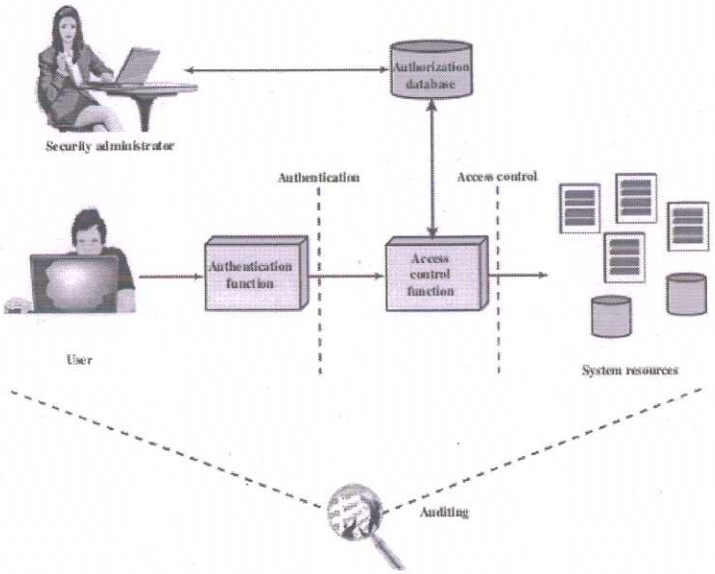
SCHEME OF EVALUATION
(Scoring Indicators)

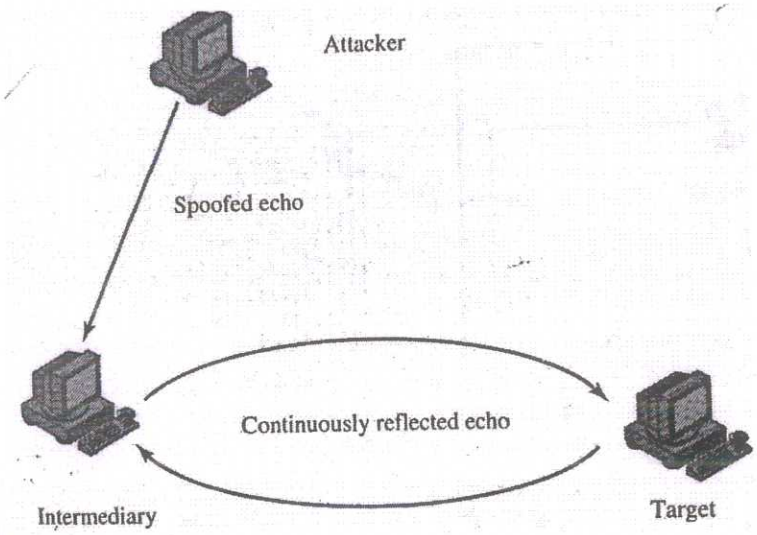
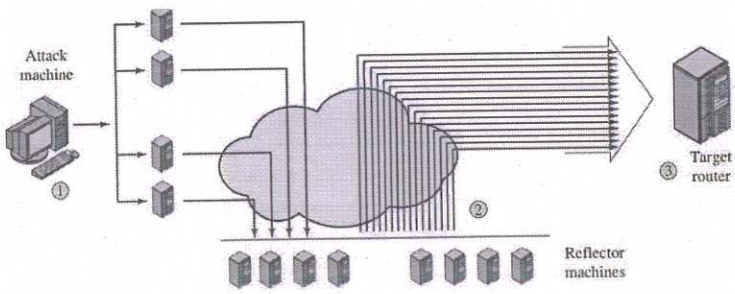
Revision : 2015		**Course code: 5136**		
Course Title : Information Security				
Q:No	**Scoring Indicator**	**Split up score**	**Sub total**	**Total**
I (1)	**PART-A** Symmetric encryption is a type of encryption where only one key (a secret key) is used to both encrypt and decrypt electronic information	2	2	2
I (2)	Finger print, iris, voice, face recognition (any four)	0.5 x 4	2	2
I (3)	The prevention of unauthorized use of a resource.	2	2	2
I (4)	This collect the data of behavior of legitimate users for a period of time Threshold detection and profile based	2	2	2
I (5)	A denial of service (DoS) is an action that prevents or impairs the authorized use of networks, systems, or applications by exhausting resources such as central processing units (CPU), memory, bandwidth, and disk space.	2	2	2
II (1)	**PART-B** CIA triad - confidentiality, integrity, and availability [Explain each]	3 x 3	6	6
II (2)	MAC algorithm is a symmetric key cryptographic technique to provide message authentication. For establishing MAC process, the sender and receiver share a symmetric key K.  Explanation needed	2 2 2	6	6

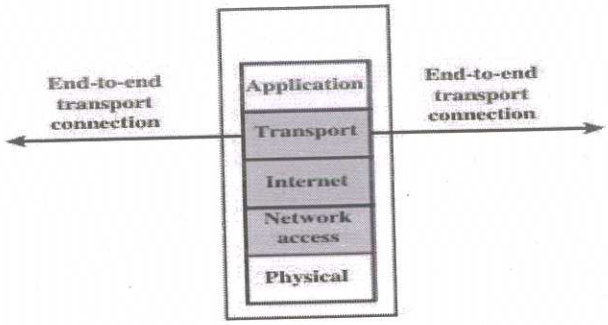
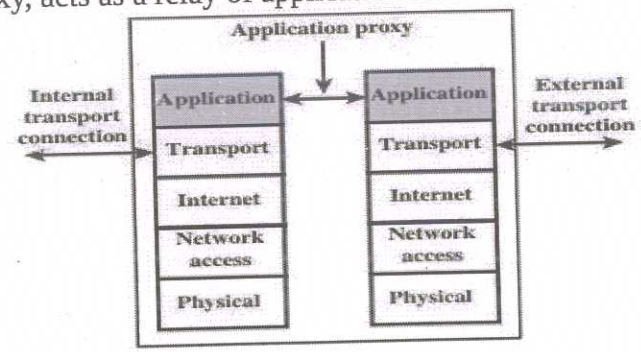
II (3)	Biometric accuracy is based on several verifying criteria including the identification rate, error rate, false acceptance rate, false alarm rate, and additional biometric system standards.  [Explanation needed]	1 3 2	6	6
II (4)	An access control policy, refers what types of access are permitted, under what circumstances, and by whom. Access control policies are generally grouped into the following categories: • Discretionary access control (DAC): Here, the access control is determined by the user with permission.ie, Controls access based on the identity of the requestor and on access rules. • Mandatory access control (MAC): Here, the administrator manages the access controls.ie, Controls access based on comparing security labels with security clearances . • Role-based access control (RBAC): This is a method of access security that is based on a person's role within a business.	3 x 3	6	6
II (5)	Snort is an open source, highly configurable and portable host-based or network-based IDS. • Detection engine • Logger • Alerter [Explain each]	1 3 2	6	6

				
II (6)	a program that secretly takes over another Internet attached computer and then uses that computer to launch or manage attacks that are difficult to trace to the bot's creator. Uses- • Distributed denial-of-service (DDoS) attacks • Spamming • Sniffing traffic • Keylogging • Spreading new malware • Installing advertisement add-ons and browser helper objects • Attacking IRC chat networks • Manipulating online polls/games [Explain any five]	1 5	6	6
II (7)	A bastion host is a system identified by the firewall administrator as a critical strong point in the network's security. The bastion host hardware platform executes a secure version of its operating system. • Only the services that the network administrator considers essential are installed on the bastion host. These could include proxy applications for DNS, FTP, HTTP, and SMTP. • The bastion host may require additional authentication before a user is allowed access to the proxy services. • Each proxy is configured to allow access only to specific host systems. • Each proxy is independent of other proxies on the bastion host.	1 5	6	6
	PART-C			

III (a)	 [Explanation needed]	4 5	9	9
I III (b)	• specification/policy • implementation/mechanisms • correctness/assurance [Explain each]	2 x 3	6	6
IV (a)	One way hash function is a mathematical function which takes a variable-length input string and converts it into a fixed-length binary sequence.  [Explanation needed]	1 3 5	9	9
IV (b)	Block Cipher and Stream Cipher are the methods used for converting the plain text into cipher text directly and belong to the family of symmetric key ciphers. • the block cipher encrypts and decrypts a block of the text at a time. • stream cipher encrypts and decrypts the text by taking the one byte of the text at a time.	2 4	6	6

	• Complexity – block: simple, stream: complex • no. of bits – block: 64 or more, stream: 8 bits			
V (a)	• Workstation hijacking • Exploiting user mistakes • Offline dictionary attack • Specific account attack • Popular password attack [Explain any three with counter measures]	3 x 3	9	9
V (b)	• Memory card • smart card • USB dongle	2 x 3	6	6
VI (a)	An access control mechanism mediates between a user and system resources  [Explanation needed]	1 4 4	9	9
VI (b)	Access control implements a security policy that specifies who have access to system resources. Following are the functions of access control:- • Authentication : Verification that the credentials of a user or other system entity are valid. • Authorization : The granting of a right or permission to a system entity to access a system resource. This function determines who is trusted for a given purpose. • Audit : An independent review and examination of system records and activities.	2 x 3	6	6
VII	Host-based IDSs (HIDSs) add a specialized layer of security software to vulnerable systems. • Anomaly detection - Threshold detection, Profile	15	15	15

	based • Signature detection - Rule-based anomaly detection, Rule-based penetration identification [Explain each briefly]			
VIII (a)	• Generic Decryption • Digital Immune System • Behavior-Blocking Software [Explain each briefly]	3 x 3	9	9
VIII (b)	Viruses, logic bombs,and backdoors,worms and bot programs [Explain any three briefly]	2 x 3	6	6
IX (a)	Reflection Attacks The attacker sends packets to a known service on the intermediary with a spoofed source address of the actual target system.  Amplification Attacks • Same as reflection attacks • differ in generating multiple response packets for each original packet sent.  	5 5	10	10

IX (b)	A common characteristic of packets used in many types of DoS attacks is the use of forged source addresses. This is known as source address spoofing. [Explanation needed]	2 3	5	5
X (a)	A packet filtering firewall applies a set of rules to each incoming and outgoing IP packet and then forwards or discards the packet.  [Brief explanation needed] An application-level gateway, also called an application proxy, acts as a relay of application-level traffic.  [Brief explanation needed]	1 2 2 1 2 2	5 5	10
X (b)	Advantages • isolates computer from external threats • Monitors Traffic • Blocks Trojans • Stops Hackers • Stops Keyloggers [Any five advantages with short description]	1 x 5	5	5