INSTITUTE OF AERONAUTICAL ENGINEERING

(Autonomous)

Dundigal, Hyderabad - 500 043

INFORMATION TECHNOLOGY

QUESTION BANK

Course Title	**INFORMATION SECURITY**				
Course Code	AITB22				
Program	B.Tech				
Semester	VI	IT/CSE			
Course Type	Elective				
Regulation	IARE - R18				
Course Structure	Theory			Practical	
	Lecture	Tutorials	Credits	Laboratory	Credits
	3	-	3	-	-
Course Coordinator	Dr. P L Srinivasa Murthy, Professor				

COURSE OBJECTIVES:

The students will try to learn:

I	Understand 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

QUESTION BANK:

Q.No	**QUESTION**	**Taxonomy**	**How does this subsume the level**	**CO’s**
MODULE I				
ATTACKS ON COMPUTERS AND COMPUTER SECURITY				
PART A-PROBLEM SOLVING AND CRITICAL THINKING QUESTIONS				
1	Enumerate Caesar cipher? And calculate the encryption and decryption for the following plain text P=”MEET ME” by using caser cipher with Key k =3?	Apply	The learner has to recall the concept of Caesar cipher. Calculate the encryption and decryption for the given plain text with given key.	CO 1
2	Interpret and contrast all kinds of cipher techniques in the cryptography?	Understand	The learner has to know all kinds of cipher techniques in the cryptography.	CO 1
3	Explain the following plain text message P=”Hide the gold in the tree stump” into cipher text with key k=”play fair example” by using play fair cipher technique?	Apply	The learner has to recall the concept of cipher text. Calculate by using play fair cipher technique given plain text.	CO 1
4	Indicate the following plain text P=”Come To School” into cipher text by using Hill cipher with key K= 3?	Understand	The learner has to recall the concept of cipher text by using hill cipher by given plain text.	CO 1
5	Find the following plaintext message P=” cryptography provides High security ”into cipher text by using simple column or transposition technique a) Basic technique b) With multiple rounds	Understand	The learner has to recall the concept of cipher text by using simple columnar transposition techniques they are basic technique, with multiple rounds.	CO 1

6	Compare and contrast all kinds of cipher techniques in the cryptography?	Understand	The learner has to know all kinds of cipher techniques in the cryptography.	CO 1
7	In Interpret the following plain text message P=”we are discovered save yourself” into ciphertext with key K=”deceptive” with key repetition?	Understand	The learner has recall the concept of cipher text with key repetition with the given plain text.	CO 1
8	Explain in details about the following: a) security attacks b) security services c) security mechanism d) plain text e) cipher text f) substitution techniques g) transposition techniques	Understand	The learner has to recall the concept of security attacks, security services, security mechanism, plain text, cipher text, substitution techniques, and transposition techniques.	CO 1
9	Focus on key range and key size, possible types of attacks?	Analyze	The learner has to know key range and key size and possible types of attacks.	CO 1
10	Illustrate transposition techniques and substitution techniques?	Analyze	The learner has to recall the concepts of transposition techniques and substitution techniques.	CO 1
PART-B LONG ANSWER QUESTIONS				
1	Explain security attacks, security services and security mechanisms with neat diagrams?	Understand	The learner has to recall the concepts security attacks, security services and security mechanisms with neat diagrams.	CO 1
2	Classify cryptanalysis and explain the amount of information known to cryptanalytic? What is cryptanalysis?	Understand	The learner has to identify cryptanalysis and has to know information about cryptanalytic. Recall the concept of cryptanalysis.	CO 1

3	Illustrate model for inter network security with neat diagram?	Understand	The learner has to recall the concept internetwork security and know model for internetwork security with neat diagram.	CO 1
4	Summarize various types of transposition techniques?	Understand	The learner has to know and identify various types of transposition techniques.	CO 1
5	Illustrate Caesar cipher? And calculate the encryption and decryption for the plain text p=" COME TO MY HOME" by using caser cipher with key=3?	Understand	The learner has to recall the concept of Caesar cipher. Calculate the encryption and decryption for the given plain text with given key.	CO 1
6	Why we use transposition techniques in cryptography?	Understand	The learner has to recall the concept of cryptography and know the use of transposition techniques.	CO 1
7	Recognize possible types of attacks?	Understand	The learner has to recall the concept of attacks and has to know types of attacks.	CO 1
8	Summarize 1. Transposition techniques 2. Steganography	Apply	The learner has to recall the concept of Transposition techniques and steganography.	CO 1
9	Describe the following a) Security attacks b) Security mechanisms	Understand	The learner has to recall the concepts security attacks and security mechanisms.	CO 1
10	Explain various types of security attacks?	Apply	The learner has to know security attacks and identify various types of security attacks.	CO 1
11	Classify cipher techniques in cryptography?	Apply	The learner has to know cryptography and cipher techniques in cryptography	CO 1
12	Distinguish plain text and cipher text?	Understand	The learner has to identify plain text and cipher text.	CO 1

13	State the following plain text P=”TRUST MEE” into cipher text by using Hill cipher with key K= which is a 2X2 matrix (only encryption)?	Remember	The learner has to recall the concept of cipher text by using hill cipher. Calculate the encryption for the given plain text.	CO 1
14	Describe the following plain text message P=”THIS IS NOT A GOLD” into cipher text with key k=”play fair example” by using playfair cipher technique?	Understand	The learner has to recall the concept cipher text by play fair cipher technique.	CO 1
15	Outline the following plain text P=”COME NOW” into cipher text by using one-time pad cipher(Vernam cipher) with key K=”NCBTZQARX”?	Understand	The learner has to recall the concept of cipher text. By using one-time pad cipher by given plain text.	CO 1
16	Identify the following plain text message P=1110001 into cipher text by using one- time pad cipher with key K=1011001.calculate both encryption and decryption for the above message?	Understand	The learner has to recall the concept of cipher text by one-time pad cipher. Calculate the encryption and decryption for the given plain text.	CO 1
17	Interpret poly-alphabetic ciphers with examples and its applications?	Analyze	The learner has to recall the concept poly-alphabetic ciphers with example and know the applications.	CO 1
18	Recall plain text, ciphers text, symmetric and asymmetric key cryptography?	Remember	The learner has to recall the concepts plain text, ciphers text, symmetric and asymmetric key in cryptography.	CO 1
19	Explain security mechanisms and a model for network security?	Understand	The learner has to know the concept of security mechanisms and a model for network security.	CO 1
20	Distinguish Caesar cipher and mono- alphabetic ciphers with examples?	Understand	The learner has to recall the concept of Caesar cipher and mono-alphabetic ciphers with examples.	CO 1

PART-C SHORT ANSWER QUESTIONS				
1	Recall the term security attacks?	Remember	The learner has to recall the concept security attacks.	CO 1
2	Define traffic analysis?	Remember	The learner has to know definition of traffic analysis and about traffic analysis.	CO 1
3	Describe Categorize active attacks?	Understand	The learner has to know active attacks and identify the categories of active attacks.	CO 1
4	List briefly categories of security mechanisms?	Remember	The learner has to recall the concept security mechanisms and has to identify the categories of security mechanisms.	CO 1
5	Compare and Distinguish active and passive attacks?	Understand	The learner has to know the definition of active and passive attacks, differences examples.	CO 1
6	Relate the key principles of security?	Understand	The learner has to identify the key principles of security.	CO 1
7	Illustrate symmetric and asymmetric encryption?	Understand	The learner has to recall the concept symmetric and asymmetric encryption.	CO 1
8	Explain the need for security?	Understand	The learner has to know the needs of security and definition of security.	CO 1
9	State Guass law and define Gaussian surface.	Remember	The learner has to know the basics tasks of security services and explain about security services.	CO 1
10	State basic tasks for defining a security services?	Remember	The learner has to recall the concept of steganography.	CO 1
11	How the mechanisms implemented for confidentiality?	Remember	The learner has to recall the concept of mechanisms and know how to implement it for confidentiality.	CO 1
12	Classify key range and key size?	Understand	The learner has identify key range and key size. CO 1	
13	Recall the term passive attacks?	Remember	The learner has to recall the concept passive attacks.	CO 1
14	Define cryptanalysis?	Remember	The learner has to know the concept cryptanalysis.	CO 1

15	Define cryptanalysis?	Understand	The learner has to know about network security and specify a model.	CO 1
16	Define security approaches?	Remember	The learner has to recall the concept security approaches.	CO 1
17	Distinguish substitution techniques and transposition techniques?	Remember	The learner has to identify the substitution techniques and transposition techniques.	CO 1
18	Compare encryption and decryption?	Understand	The learner has to recall the concept encryption and decryption. Identify encryption and decryption.	CO 1
19	How transposition techniques differ from substitution techniques?	Remember	The learner has to identify transposition techniques from substitution techniques.	CO 1
20	Convert Cartesian co-ordinates to cylindrical co-ordinates.	Remember	The learner has to know various security approaches.	CO 1
MODULE II				
SYMMETRIC KEY CIPHERS				
PART-A PROBLEM SOLVING AND CRITICAL THINKING QUESTIONS				
1	Describe why it is important to study the feistel cipher?	Understand	The learner has to know why it is important to study the feistel cipher.	CO 2
2	Distinguish between diffusion and confusion in the cryptography?	Understand	The learner has to identify diffusion and confusion in the cryptography	CO 2
3	Discover DES the first 24 bits of each sub key come from the same subset of 28 bits of the initial key and that the second 24 bits of each sub key come from a disjoint subset of 28bit initial key?	Apply	The learner has to calculate DES the first 24 bits of each sub key come from the same subset of 28 bits of the initial key and that the second 24 bits of each sub key come from a disjoint subset of 28 bit initial key.	CO 2
4	Explain why do some block cipher modes of operation only use encryption while others use both encryption and decryption?	Understand	The learner has to know why do some block cipher modes of operation only use encryption while others use both encryption and decryption.	CO 2

5	Describe the purpose of the S-boxes in DES?	Analyze	The learner has to recall the concept DES and know the purpose of the S- boxes in DES.	CO 2
6	Illustrate if a bit error occurs in the transmission of a cipher text character in 8- bit CFB mode how far does the error propagate?	Apply	The learner has to know if a bit error occurs in the transmission of a cipher text character in 8- bit CFB mode how far does the error propagate.	CO 2
7	Explain different types of stream ciphers with neat diagrams?	Understand	The learner has to identify types of stream ciphers with neat diagrams.	CO 2
8	Examine which parameters and design choices determine the actual algorithm of a feistel cipher?	Apply	The learner has to know which parameters and design choices determine the actual algorithm of a feistel cipher.	CO 2
9	Explain differential and linear cryptanalysis?	Apply	The learner has to recall the concepts differential and linear cryptanalysis.	CO 2
10	Interpret diffusion and confusion in the cryptography?	Understand	The learner has to know diffusion and confusion in the cryptography.	CO 2
PART-B LONG ANSWER QUESTIONS				
1	Distinguish between AES and DES in a brief manner?	Understand	The learner has to identify AES and DES.	CO 2
2	Write how DES algorithm uses feistel cipher structure?	Understand	The learner has to recall the concept DES algorithm and feistel cipher structure to know how DES algorithm uses feistel cipher structure.	CO 2
3	Demonstrate how encryption is misused to attack the system?	Understand	The learner has to know how encryption is misused to attack the system.	CO 2
4	Explain Diffie- Hellman algorithm?.	Understand	The learner has to recall the concept Diffie-Hellman algorithm.	CO 2
5	Find how the placement of encryption will works?	Understand	The learner has to known how the placement of encryption will work.	CO 2

6	Illustrate how Compile the process how RC4 decryption is reverse of its encryption?	Understand	The learner has to know how to compile a process and how RC4 decryption is reverse of its encryption.	CO 2
7	Recall the principles of conventional encryption algorithms?	Understand	The learner has to recall the concept of conventional encryption algorithms and its principles.	CO 2
8	Demonstrate how the placement of encryption will works?.	Understand	The learner has to know how the placement of encryption will work.	CO 2
9	Find Recite round function evaluation in feistel cipher structure?	Understand	The learner has to recall the concept of feistel cipher structure and find recite round function evaluation in feistel cipher structure.	CO 2
10	Demonstrate how key is distributed in the RSA algorithm?	Understand	The learner has to recall the concept RSA algorithm and how key is distributed in the RSA algorithm.	CO 2
11	How diffusion and confusion increases complexity to thwart the cryptanalyst?	Understand	The learner has to know diffusion and confusion increases complexity to thwart the cryptanalyst.	CO 2
12	Explain elliptic curve cryptography?	Understand	The learner known elliptic curve cryptography.	CO 2
13	Recall linear and differential cryptanalysis in a detail manner?	Understand	The learner has to recall the concept linear and differential cryptanalysis.	CO 2
14	Recall Blowfish, AES and RC4?	Understand	The learner has to recall the concept BlowFish, AES, and RC4.	CO 2
15	Identify all the principles of the public key crypto systems?	Understand	The learner has to identify all the principles of the public key crypto systems.	CO 2
16	Explain briefly about RSA algorithm and ECC in a detail manner?	Understand	The learner has to know RSA algorithm and ECC.	CO 2
17	Explain AES encryption and decryption process with neat sketch?	Understand	The learner has to know AES encryption and decryption process with neat sketch.	CO 2

18	Discuss key distribution of Asymmetric key Ciphers?	Understand	The learner has to identify key distribution of asymmetric key ciphers.	CO 2
19	Enumerate differential cryptanalysis?	Understand	The learner has to recall the concept of differential cryptanalysis.	CO 2
20	Describe stream ciphers?	Understand	The learner has to know stream ciphers.	CO 2
PART-C SHORT ANSWER QUESTIONS				
1	Explain stream and block ciphers with examples?	Remember	The learner has to recall the concept stream and block ciphers with examples.	CO 2
2	Identify DES, AES, Blowfish algorithms?	Understand	The learner has to know DES, AES, Blowfish algorithms.	CO 2
3	List out block cipher modes of operation?	Remember	The learner has to identify block cipher modes of operation.	CO 2
4	Recall product cipher?	Remember	The learner has to recall the concept of product cipher.	CO 2
5	Summarize design parameters of feistel cipher structure?	Understand	The learner has to know design parameters of feistel cipher structure and recall the concept feistel cipher structure.	CO 2
6	Why is symmetric-key cryptography important?	Remember	The learner has to identify symmetric- key cryptography and its importance.	CO 2
7	Why is symmetric-key cryptography used?	Understand	The learner has to recall the concept symmetric-key in cryptography and its uses.	CO 2
8	Name RC4 Location?	Remember	The learner has to identify RC4 Location.	CO 2
9	Show advantages of ciphers modes of operation?	Understand	The learner has to recall the concepts of ciphers modes of operation and its advantages.	CO 2
10	Recall Differential and Linear Cryptanalysis?	Remember	The learner has to identify differential and linear cryptanalysis.	CO 2
11	Recall the steps in AES algorithms?	Understand	The learner has to recall the steps in AES algorithms.	CO 2

12	Explain RC4 Location?	Understand	The learner has to recall the concept RC4 Location.	CO 2
13	Explain the procedure for DES algorithm?	Understand	The learner has to know the procedure for DES algorithm	CO 2
14	Explain the procedure for RSA algorithm?	Understand	The learner has to know the procedure for RSA algorithm.	CO 2
15	Illustrate RSA Diffie-Helmann, ECC Key Distribution Algorithm?	Remember	The learner has to recall the concept of RSA Diffie-Helmann ECC Key Distribution Algorithm.	CO 2
16	List key distribution Asymmetric key Ciphers?	Remember	The learner has to identify the key distribution asymmetric key ciphers.	CO 2
17	Demonstrate link and end-to-end encryption?	Remember	The learner has to recall the concept of link and end-to-end encryption.	CO 2
18	Recall session key and master key?	Understand	The learner has to recall the concept of session key and master key.	CO 2
19	Recall the design criteria of block cipher?	Remember	The learner has to know about the design criteria of block cipher.	CO 2
20	Write placement of encryption function?	Remember	The learner has to identify the placemsent of encryption function.	CO 2
MODULE III				
MESSAGE AUTHENTICATION ALGORITHM AND HASH FUNCTIONS				
PART A-PROBLEM SOLVING AND CRITICAL THINKING QUESTIONS				
1	Demonstrate what changes in HMAC are required in order to replace one underlying hash function with another?	Apply	The learner has to know what changes in HMAC are required in order to replace one underlying hash function with another.	CO 3
2	Compare the differences between MD4 and MD5.specifically, to what extent? Do you think that MD5 is stronger than MD4, and why?	Apply	The learner has to identify MD4 and MD5 and to know MD5 is stronger than MD4.	CO 3

3	Illustrate what types of attacks are addressed by message authentication?	Apply	The learner has to identify types of attacks are addressed by message authentication.	CO 3
4	Demonstrate why has there been an interest in developing a message authentication code derived from a cryptographic hash function as opposed to one derived from a symmetric cipher?	Apply	The learner has to know why has there been an interest in developing a message authentication code derived from a cryptographic hash function as opposed to one derived from a symmetric cipher.	CO 3
5	Examine what basic arithmetical and logical functions are used in MD5?	Apply	The learner has to recall basic arithmetical and logical functions are used in MD5	CO 3
6	What is digital signature? Explain in detail?	Apply	The learner has to recall digital signature.	CO 3
7	Illustrate types of attacks are addressed by message authentication?	Apply	The learner has to identify types of attacks are addressed by message authentication.	CO 3
8	Illustrate some approaches to producing message authentication?	Apply	The learner has to know some approaches to producing message authentication.	CO 3
9	Interpret what characters are needed in a secure hash function?.	Apply	The learner has to identify what characters are needed in a secure hash function.	CO 3
10	Examine public key infrastructure?	Apply	The learner has to recall the concept public key infrastructure.	CO 3
PART-B LONG ANSWER QUESTIONS				
1	Explain secure hash algorithms protocol?	Understand	The learner has to know secure hash algorithms protocol.	CO 3
2	Outline the following terms in detail a) whirlpool b) knapsack algorithm	Understand	The learner has to recall whirlpool and knapsack algorithm.	CO 3

3	Explain knapsack algorithm with an example?	Understand	The learner has to know knapsack algorithm with an example.	CO 3
4	Define biometric authentication and how it is important to support security in real time and suggest your answer?	Understand	The learner has to recall the concept biometric authentication and its importance to support security in real time.	CO 3
5	How X.509 certificate is revoked?	Understand	The learner has to know X.509 certificate is revoked.	CO 3
6	Discuss the message digest function in digital signatures with an example?	Understand	The learner has to know the message digest function in digital signatures with an example.	CO 3
7	Create whirlpool mechanism with an example?	Understand	The learner has to recall whirlpool mechanism with an example.	CO 3
8	ExplainX.509 certificates with neat diagram?	Understand	The learner has to know X.509 certificates with neat diagram.	CO 3
9	Demonstrate briefly what are the different kinds of the authentication requirements are there for message authentication?	Understand	The learner has to identify different kinds of the authentication requirements are there for message authentication.	CO 3
10	Differentiate public key and private key and explain public key infrastructure with an example?	Understand	The learner has to recall public key and private key and know public key infrastructure with example.	CO 6
11	Explain Kerberos v4 and Kerberos v5?	Understand	The learner has to know Kerberos v4 and Kerberos v5.	CO 3
12	Describe the Kerberos security mechanism and explain why it is important in real time for providing security?	Understand	The learner has to identify the Kerberos security mechanism and why it is important in real time for providing security.	CO 3
13	Which Kerberos is more secure than the other security mechanisms?	Understand	The learner has to know which Kerberos is more secure than the other security mechanisms.	CO 3

14	Calculate the values of W16, W17, W18, W19. Explain SHA-1?	Apply	The learner has to calculate the values of W16, W17, W18, W19 and recall the concept SHA-1.	CO 3
15	What are the different types of the message authentication codes and explain with an example?	Remember	The learner has to identify types of the message authentication codes and with example.	CO 3
16	Define X.509 certificates with neat diagram?	Understand	The learner has to know X.509 certificates with neat diagram.	CO 3
17	Explain authentication service? Explain x.509 authentication services in a detail manner?	Understand	The learner has to recall the concept authentication service and Explain x.509 authentication services.	CO 3
18	Briefly explain hash functions?	Understand	The learner has to recall the concept hash function.	CO 3
19	Bring digital signatures with an example?	Understand	The learner has to recall the concept digital signatures with example.	CO 3
20	Illustrate management functions of PKIX and describe the process in public Key infrastructure?	Understand	The learner has to know management functions of PKIX and the process in public Key infrastructure.	CO 3
PART-C SHORT ANSWER QUESTIONS				
1	Distinguish HMAC and CMAC?	Understand	The learner has to identify HMAC and CMAC.	CO 3
2	Recall Authentication requirements?	Understand	The learner has to recall concept Authentication requirements.	CO 3
3	List authentication codes?	Remember	The learner has to recall the concept authentication codes.	CO 3
4	Recall HMAC?	Understand	The learner has to know HMAC.	CO 3
5	Define CMAC?	Understand	The learner has to know CMAC.	CO 3
6	Show Secure hash algorithm?	Remember	The learner has to recall secure hash algorithm.	CO 3
7	Explain the steps in knapsack algorithm?	Remember	The learner has to know the steps in knapsack algorithm.	CO 3
8	What is message digest?	Understand	The learner has to know message digest.	CO 3

9	Recall Public – Key Infrastructure?	Understand	The learner has to recall the concept Public – Key Infrastructure.	CO 3
10	Define digital signatures?	Remember	The learner has to know digital signature.	CO 3
11	Choose key principles of Biometric Authentication?	Understand	The learner has to recall the concept Biometric Authentication and its key principles.	CO 3
12	Explain about X.509 certificate?	Remember	The learner has to know X.509 certificate.	CO 3
13	Recall message authentication applications?	Understand	The learner has to recall the concept of message authentication and its applications.	CO 3
14	Define simple and secure authentication dialogue in Kerberos?	Remember	The learner has to know simple and secure authentication dialogue in Kerberos.	CO 5
15	Illustrate X.509 services?	Understand	The learner has to know X.509 services.	CO 3
16	Explain private and public key?	Understand	The learner has to recall the concept of private and public key.	CO 3
17	What is MD4 and MD5?	Understand	The learner has to know MD4 and MD5.	CO 3
18	Suppose what is message authentication algorithm?	Understand	The learner has to know what is message authentication algorithm.	CO 3
19	DifferentiateMD4 and MD5?	Remember	The learner has to identify MD4 and MD5.	CO 3
20	What is simple and secure authentication?	Understand	The learner has to recall the concept simple and secure authentication.	CO 3

MODULE IV				
E-MAIL SECURITY				
PART A- PROBLEM SOLVING AND CRITICAL THINKING QUESTIONS				
1	Discuss why PGP generate a signature before remembering?	Understand	The learner has to recall the concept PGP and to know why PGP generate a signature before remembering.	CO 4
2	Explain why is R64 conversion is useful for an e-mail application?	Understand	The learner has to know why is R64 conversion is useful for an e-mail application.	CO 4
3	Discuss the examples of applications of IPSec?	Understand	The learner has to recall the concept IPSec and its applications.	CO 4
4	Examine what are the services provided by IPSec?	Apply	The learner has to recall the concept IPSec and to know what are the services provided by IPSec.	CO 4
5	Distinguish the differences between MIME and SIMIME?	Analyze	The learner has to identify MIME and SIMIME.	CO 4
6	Examine and support your answer how PGP use the concept of trust?	Apply	The learner has to know how PGP use the concept of trust.	CO 4
7	Explain what parameters to identify an SA and what parameters characterize the nature of particular SA?	Analyze	The learner has to know what parameters to identify an SA and what parameters characterize the nature of particular SA.	CO 4
8	Summarize why is the segmentation and reassembly function in PGP?	Understand	The learner has to identify why the segmentation and reassembly function in PGP is.	CO 4
9	Write about the basic approaches to bundling SAs?	Apply	The learner has to identify the basic approaches to bundling SAs.	CO 4
10	Explain why does ESP Implement a padding field?	Analyze	The learner has to recall the concept ESP and to know a padding field.	CO 4
PART-B LONG ANSWER QUESTIONS				
1	Explain MIME specification with an example?	Understand	The learner has to recall the concept MIME and its specification.	CO 4

2	Infer out the general format of PGP message with an example?	Understand	The learner has to recall the concept PGP and to know the general format of PGP message.	CO 4
3	Describe the general structure of Oakley key?	Understand	The learner has to recall the concept Oakley key with the general structure.	CO 4
4	Explain all services of PGP and explain with neat sketch?	Understand	The learner has to recall the concept PGP.	CO 4
5	Estimate on what basis Zimmermann has developed PGP fore-mail security?	Understand	The learner has to know on what basis Zimmermann has developed PGP for e-mail security.	CO4
6	Explain IP security overview?	Understand	The learner has to recall the concept IP security with overview.	CO 4
7	Describe and explain how the security will be provided in Email?	Understand	The learner has to know how the security will be provided in Email.	CO 4
8	Extend the Discuss about the IP security architecture in detail?	Understand	The learner has to identify IP security architecture in detail.	CO 4
9	Discuss about the key management in email security?	Understand	The learner has to recall the concept key management in email security.	CO4
10	Illustrate about the MIME content types?	Understand	The learner has to know and identify MIME content types.	CO4
11	Classify the Combining Security associations?	Analyze	The learner has to know Combining Security associations.	CO 4
12	Explain MIME transfer encoding techniques and certificate processing?	Understand	The learner has to identify MIME transfer encoding techniques and certificate processing.	CO 4
13	Illustrate ISAKMP key management?	Understand	The learner has to know ISAKMP key management.	CO 4
14	Evaluate the importance of the authentication header and explain its structure?	Analyze	The learner has to analyze the importance of the authentication header and explain its structure.	CO 4
15	Explain SIMIME message?	Understand	The learner has to recall the concept SIMIME message.	CO 4

16	Illustrate how encapsulating security payload is defined?	Understand	The learner has to know about security payload and its importance.	CO 4
17	Explain combining security associations?	Understand	The learner has to how encapsulating security payload is defined.	CO 4
18	Describe the importance of the authentication header and explain its structure?	Understand	The learner has to know the importance of the authentication header and explain its structure.	CO 4
19	Interpret why SIMIME is a security enhancement to MIME internet email format standard?	Apply	The learner has to identify why SIMIME is a security enhancement to MIME internet email format standard.	CO 4
20	Discuss why in spite of symmetric key, public key and private key, uses three separate requirements what are those and explain why are used?	Understand	The learner has to analyze why in spite of symmetric key, public key and private key, uses three separate	CO 4
PART-C SHORT ANSWER QUESTIONS				
1	Recall the term PGP?	Remember	The learner has to recall the concept PGP	CO 4
2	Visualize the terms IP Security and Authentication Header?	Remember	The learner has to identify the terms IP Security and Authentication Header.	CO 6
3	Explain why PGP is open source?	Understand	The learner has to know PGP in open source.	CO 4
4	Tabulate notations used in PGP?	Remember	The learner has to know the notations used in PGP.	CO 4
5	Distinguish PGP and MIME types?	Understand	The learner has to identify PGP and MIME types.	CO 4
6	Summarize e-mail compatibility?	Understand	The learner has to know e-mail compatibility.	CO 6
7	Recall services of PGP?	Remember	The learner has to recall the concept services of PGP.	CO 4
8	Illustrate about IP Security?	Understand	The learner has to know IP Security.	CO 6
9	Express what do you understand by encapsulating Security payload?	Understand	The learner has to recall the concept of encapsulating Security payload.	CO 6

10	Demonstrate why does PGP generate a signature before Remembering?	Understand	The learner has to recall the concept PGP and know why does PGP generate a signature before Remembering.	CO 6
11	Describe the over view of security?	Understand	The learner has to know the over view of security.	CO 6, CO 7
12	Define the architecture of IP Security?	Remember	The learner has to know architecture of IP Security.	CO 6
13	Describe how does PGP provide public key management?	Remember	The learner has to recall the concept PGP and know how does PGP provide public key management.	CO 4
14	Illustrate the utility of a detached signature?	Understand	The learner has to know the utility of a detached signature.	CO 6
15	Generalize IP Security overview?	Understand	The learner has to recall the concept IP Security and to know IP Security overview.	CO 6
16	Distinguish Header and PGP?	Understand	The learner has to identify Header and PGP.	CO 6
17 hline 18	Define Authentication Header? Recall key management?	Remember Remember	The learner has to know Authentication Header. The learner has to recall the concept key management.	CO 4 CO 4
19	Explain encapsulating Security payload?	Understand	The learner has to know encapsulating Security payload.	CO 4
20	Express the over view of security?	Understan	d The learner has to know the over view of security.	CO 6
MODULE V				
WEB SECURITY				
PART A-PROBLEM SOLVING AND CRITICAL THINKING QUESTIONS)				
1	In SSL and TLS? Illustrate why is there a separate change cipher Spec protocol rather than including a change cipher- Spec message in the Handshake protocol?	Analyze	The learner has to recall the concepts of SSL and TLS and to know why is there a separate change cipher Spec protocol rather than including a change cipher-Spec message in the Handshake protocol.	CO 5

2.	Describe about the cross sire scripting vulnerability?	Understand	The learner has to know cross sire scripting vulnerability.	CO 5
3	Justify Intrusion provides early warning of an intrusion so that action can be taken to prevent or minimize damage?	Analyze	The learner has to know Intrusion provides early warning of an intrusion so that action can be taken to prevent or minimize damage.	CO 5
4	Illustrate the principal categories of SET participants?	Apply	The learner has to recall the concept SET and its principle and categories of SET participants.	CO 5
5	Illustrate the parameters that define an SSL session state?	Analyze	The learner has to know the parameters that define an SSL session state.	CO 5
6	Define and Discuss three classes of intruders?	Understand	The learner has to identify three classes of intruders.	CO 5
7	Discuss what are the two common techniques used to protect a password file?	Understand	The learner has to know the two common techniques used to protect a password file.	CO 5
8	Classify how does a worm propagate?	Understand	The learner has to identify how a worm propagates.	CO 5
9	Evaluate statistical anomaly detection is different from rule based intrusion?	Analyze	The learner has to know and identify statistical anomaly detection is different from rule based intrusion.	CO 5
10	Describe dual signature and its purpose?	Understand	The learner has to know dual signature and its purpose.	CO 5
PART-B LONG ANSWER QUESTIONS				
1	Explain how does the intrusion detection system work when the contents of the network message are encrypted? At what level can this packet be read and analyzed?	Understand	The learner has to know how does the intrusion detection system work and the contents of the network message are encrypted.	CO 5
2	Discuss how hackers exploit vulnerabilities in the network-based computing systems?	Understand	The learner has to recall the concept network-based computing systems and how hackers exploit vulnerabilities.	CO 5

3	Distinguish socket layer security and transport security?	Understand	The learner has to identify socket layer security and transport security.	CO 5
4	Distinguish statistical anomaly detection and rule–based intrusion detection?	Understand	The learner has to identify statistical anomaly detection and rule–based intrusion detection.	CO 5
5	Generalize the different types of the secure electronic transaction?	Understand	The learner has to identify types of the secure electronic transaction.	CO 6
6	Summarize counter measure for viruses and worms?	Understand	The learner has to know counter measure for viruses and worms.	CO 6
7	Describe the firewall design principles in a detail manner?	Understand	The learner has to recall the concept firewall design and its principles.	CO 5
8	Explain various approaches to prevention and detection from users?	Understand	The learner has to identify various approaches to prevention and detection from users.	CO 5
9	Describe standard approach to the protection of local computer assets external threats?	Understand	The learner has to know standard approach to the protection of local computer assets external threats.	CO 6
10	Explain software threats to systems with a special emphasis on viruses and worms?	Understand	The learner has to recall the concept viruses and worms in software threats to systems with a special emphasis	CO 5
11	Explain the concept of the virtual electronics?	Understand	The learner has to recall the concept of the virtual electronics.	CO 5
12	Discuss about the cross site scripting vulnerability?	Understand	The learner has to know cross site scripting vulnerability.	CO 5
13	Describe the different types of firewalls in a detail manner?	Understand	The learner has to identify different types of firewalls.	CO 5
14	Explain different types of the viruses and firewalls in web security?	Understand	The learner has to identify different types of the viruses and firewalls in web security.	CO 5

15	Differentiate statistical anomaly detection and rule–based intrusion detection?	Understand	The learner has to identify statistical anomaly detection and rule–based intrusion detection.	CO 5
16	Explain how intrusion prevention is achieved through password management?	Understand	The learner has to know how intrusion prevention is achieved through password management.	CO 5
17	Differentiate SSL and TLS protocols?	Understand	The learner has to identify SSL and TLS protocols.	CO 5
18	Explain firewall design principles and also explain techniques?	Understand	The learner has to know firewall design and its principles and techniques.	CO 5
19	Explain how intrusion prevention is achieved through password management?	Understand	The learner has to know intrusion prevention is achieved through password management.	CO 5
20	Describe transaction? And explain the inter branch payment transactions?	Understand	The learner has to recall the concept transaction and the inter branch payment transactions.	CO 5
PART-C SHORT ANSWER QUESTIONS				
1	Recall types of viruses?	Remember	The learner has to identify types of viruses.	CO 5
2	List files access activities used for intrusion detection?	Remember	The learner has to know files access activities used for intrusion detection.	CO 5
3	Illustrate different file access activities used for intrusion detection?	Understand	The learner has to know different file access activities used for intrusion detection.	CO 5
4	Discuss in the context of access control?	Understand	The learner has to know context of success control.	CO 5
5	Recall secure socket layer and transport layer security?	Remember	The learner has to recall the concept secure socket layer and transport layer security.	CO 5
6	Recall the techniques used to avoid guessable password?	Remember	The learner has to know techniques used to avoid guessable password.	CO 5
7	Describe three benefits that can be provided by an intrusion?	Understand	The learner has to identify three benefits that can be provided by an intrusion.	CO 6
8	Illustrate how biometrics used instead of password for authentication?	Understand	The learner has to know how biometrics used instead of password.	CO 5

9	Discuss firewall and principles of firewall?	Understand	The learner has to recall the concept firewall and its principles.	CO 5
10	Discuss statistical anomaly detection and rule based intrusion?	Understand	The learner has to recall the concept statistical anomaly detection and rule based intrusion.	CO 5
11	Illustrate an application-level gateway?	Understand	The learner has to know application- level gateway.	CO 5
12	List out design goals for a firewall?	Remember	The learner has to identify design goals for a firewall.	CO 5
13	Recall packet filter routing and a state full inspection firewall?	Remember	The learner has to recall the concepts packet filter routing and a state full inspection firewall.	CO 5
14	Illustrate how firewall is different from intrusion detection system?	Understand	The learner has to identify how firewall is different from intrusion detection system.	CO 5
15	Explain protocols that comprise SSL?	Understand	The learner has to recall the concepts protocols and comprise SSL.	CO 5
16	Show alert codes of TLS protocol?	Remember	The learner has to recall the concepts alert codes of TLS protocol.	CO 5
17	Express SSL and TLS protocols?	Understand	The learner has to recall the concepts SSL and TLS protocols.	CO 6
18	Interpret parameters that define SSL session state?	Understand	The learner has to know parameters that define SSL session state.	CO 5
19	Differentiate statistical anomaly detection and rule based intrusion?	Understand	The learner has to identify statistical anomaly detection and rule based intrusion.	CO 5
20	List services provided by SSL record protocol?	Remember	The learner has to know services provided by SSL record protocol.	CO 5

Course Coordinator: **HOD IT**
Dr P L Srinivasa Murthy, Professor