INSTITUTE OF AERONAUTICAL ENGINEERING

(Autonomous)

Dundigal, Hyderabad - 500 043

INFORMATION TECHNOLOGY

TUTORIAL QUESTION BANK

Course Name	**INFORMATION SECURITY**
Course Code	**ACS013**
Class	**B. Tech VIII Semester**
Branch	**Information Technology**
Course Coordinator	**Ms B Geetavani, Assistant Professor**
Course Faculty	**Ms B Anupama, Assistant Professor** **Ms B Swathi, Assistant Professor** **Ms P Navya, Assistant Professor**

COURSE OBJECTIVIES:

The course should enable the students to:

I	Understand the basic categories of threats to computers and networks.
II	Master the implementation of various cryptographic algorithms. Be familiar with public cryptography.
III	Analyze PGP and use PGP package to send encrypted e-mail message.
IV	Interpret the operation of the protocols that are used inside the Internet.
V	Discuss the place of ethics in the information security area.

COURSE OUTCOMES:

CO1	Understand the basic concepts on attacks of computer and computer security.
CO2	Understand the concepts of symmetric key ciphers.
CO3	To describe about the message authentication algorithm and hash functions.
CO4	Understand the concepts of e-mail security.
CO5	Understand the concepts of web security.

COURSE LEARNING OUTCOMES:

Students, who complete the course, will have demonstrated the ability to do the following:

ACS013.01	Understand the different types of attacks, security mechanisms, security services.
ACS013.02	Explain Define various substitution techniques such as play-fair cipher, mono-alphabetic cipher and hill cipher.
ACS013.03	Understand various Transposition techniques such as row transposition and rail fence.
ACS013.04	Describe the role of key in encryption and key size.
ACS013.05	Apply the symmetric algorithm for message transmission and analyze the security level of it.
ACS013.06	Understand various asymmetric key encryption algorithms for message encryption and decryption.
ACS013.07	Understand the block cipher modes of operation for encryption and decryption.
ACS013.08	Describe the need of stream ciphers in message encryption.
ACS013.09	Understand the role of elliptic curve cryptography in security.
ACS013.10	Analyze the drawbacks of RSA and students will be able to design a security algorithm which overcomes that drawbacks.

ACS013.11	Explain the role of the message authentication in message transmission.
ACS013.12	Explain the need of digital signature in message transmission.
ACS013.13	Explain and demonstrate the role of different types of hash functions for providing security.
ACS013.14	Understand the differences between the symmetric and symmetric cryptography algorithms for providing security.
ACS013.15	Explain S/MIME and PGP for transmitting mail from sender to receiver.
ACS013.16	Explain IP security for internet protocol and analyze how it provides security.
ACS013.17	Describe the security socket layer and transport layer security for web security.
ACS013.18	Analyze various types of intrusion detection techniques.
ACS013.19	Describe various types of viruses and its threats.
ACS013.20	Describe various types of firewalls and analyze the security level of these.

TUTORIAL QUESTION BANK

UNIT - I

PART - A (SHORT ANSWER QUESTIONS)

S.No	Question	Blooms Taxonomy Level	Course Outcomes	Course Learning Outcomes
1.	Explain security attacks.	Remember	CO1	ACS013.01
2.	Enumerate traffic analysis?	Understand	CO1	ACS013.01
3.	Categorize active attacks.	Understand	CO1	ACS013.01
4.	Categorize passive attacks.	Understand	CO1	ACS013.01
5.	Mention the key principles of security.	Remember	CO1	ACS013.01
6.	Distinguish active and passive attacks?	Understand	CO1	ACS013.01
7.	Enumerate the mechanisms implemented for	Remember	CO1	ACS013.01
8.	List briefly categories of security mechanisms.	Understand	CO1	ACS013.01
9.	Specify basic tasks for defining a security services?	Remember	CO1	ACS013.01
10.	Differentiate symmetric and asymmetric encryption?	Remember	CO1	CAIT004.01
11.	Define cryptanalysis?	Understand	CO1	ACS013.01
12.	List various Security approaches?	Understand	CO1	ACS013.03
13.	Specify model for Network Security.	Remember	CO1	ACS013.01
14.	Explain the need for security.	Remember	CO1	ACS013.01
15.	Distinguish substitution techniques?	Understand	CO1	ACS013.01
16.	Distinguish transposition techniques?	Understand	CO1	ACS013.02
17.	Differentiate encryption and decryption?	Understand	CO1	ACS013.03
18.	Differentiate symmetric and asymmetric key	Understand	CO1	ACS013.04
19.	Define steganography.	Remember	CO1	ACS013.04
20.	Enumerate key range and key size?	Understand	CO1	ACS013.04

PART -B (LONG ANSWER QUESTIONS)

S.No	Question	Blooms Taxonomy Level	Course Outcomes	Course Learning Outcomes
1.	Explain security attacks, security services and security mechanisms with neat diagrams.	Understand	CO1	ACS013.01
2.	Define cryptanalysis? Mention the types of cryptanalysis and explain the amount of information known to cryptanalytic?	Remember	CO1	ACS013.04
3.	Demonstrate model for internetwork security with neat diagram?	Understand	CO1	ACS013.01
4.	Explain various types of transposition techniques.	Understand	CO1	ACS013.03
5.	Define Caesar cipher? And calculate the encryption and decryption for the plain text P=”COME TO MY HOME” by using caser cipher with Key k=3?	Remember	CO1	ACS013.03
6.	Convert 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	CO1	ACS013.03
7.	Convert the following plain text P=”TRUST MEE” into cipher text by using Hill cipher with key K= which is a 2X2 matrix (only encryption).	Understand	CO1	ACS013.03
8.	Explain poly-alphabetic ciphers with examples and its	Understand	CO1	ACS013.03
9.	Explain the following i) Transposition Techniques ii) Steganography	Remember	CO1	ACS013.03
10.	Explain Hill cipher with examples.	Understand	CO1	ACS013.03
11.	Explain Caesar cipher and mono-alphabetic ciphers with examples?	Remember	CO1	ACS013.03

PART -C (CRITICAL THINKING QUESTIONS)				
1.	Define Caesar cipher? And calculate the encryption and decryption for the following plain text P=”MEET ME” by using caser cipher with Key k =3?	Understand	CO1	ACS013.03
2.	Convert 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?	Understand	CO1	ACS013.03
3.	Convert the following plain text P=”Come To School” into cipher text byusing Hill cipher with key K= 3.	Understand	CO1	ACS013.03
4	Convert the following plain text message P=”I discovered a gravitational force “into cipher text by using mono alphabetic cipher technique.	Understand	CO1	ACS013.03
.	Understand and contrast all kinds of cipher techniques in the cryptography?	Remember	CO1	ACS013.02
5.	Convert the following plain text message P=”we are discovered save yourself” into cipher text with key K=”deceptive” with key repetition.	Understand	CO1	ACS013.03
6.	Convert the following plain text message P=”cryptography provides high security” into cipher text by using simple columnar transposition technique basic technique with multiple rounds.	Understand	CO1	ACS013.03
7.	Differentiate transposition techniques and substitution techniques?	Remember	CO1	ACS013.02
UNIT – II				
PART - A (SHORT ANSWER QUESTIONS)				
1.	Understand stream and block ciphers with examples?	Understand	CO2	ACS013.07
2.	Differentiate DES, AES, Blowfish algorithms?	Understand	CO2	ACS013.06
3.	Differentiate Differential and Linear Cryptanalysis?	Remember	CO2	ACS013.06
4.	Enumerate design parameters of feistel cipher structure?	Understand	CO2	ACS013.05
5.	Define product cipher?	Understand	CO2	ACS013.07
6.	Listoutblock cipher modes of operation?	Remember	CO2	ACS013.07
7.	Differentiate link and end-to-end encryption?	Understand	CO2	ACS013.06
8.	Differentiate session key and master key?	Understand	CO2	ACS013.05
9.	State advantages of counter mode?	Understand	CO2	ACS013.08
10.	Explain essential ingredients of symmetric cipher.	Understand	CO2	ACS013.05
11.	Specify the design criteria of block cipher?	Understand	CO2	ACS013.07
12.	Explain RC4 Location.	Understand	CO2	ACS013.08
13.	Enumerate placement of encryption function?	Understand	CO2	ACS013.06
14.	List key distribution Asymmetric key Ciphers?	Remember	CO2	ACS013.06
15.	Explain principles of public key cryptosystems.	Remember	CO2	ACS013.06
16.	Differentiate RSA Diffie-Helmann, ECC Key Distribution Algorithm?	Understand	CO2	ACS013.09
17.	Explain the procedure for DES algorithm.	Understand	CO2	ACS013.05
18.	List the steps in AES algorithms?	Understand	CO2	ACS013.05
19.	Explain the procedure for RSA algorithm.	Understand	CO2	ACS013.10
20.	Describe the steps in ECC Key Distribution algorithm?	Understand	CO2	ACS013.09
PART -B (LONG ANSWER QUESTIONS)				
1.	Justify how DES algorithm uses feistel cipher structure.	Remember	CO2	ACS013.05
2.	Describe how Compile the process how RC4 decryption is reverse of its encryption?	Understand	CO2	ACS013.05
3.	Enumerate the principles of conventional encryption algorithms?	Understand	CO2	ACS013.05
4.	Demonstrate how encryption is misused to attack the system?	Remember	CO2	ACS013.05
5.	Recite round function evaluation in feistel cipher structure?	Remember	CO2	ACS013.05
6.	Understand and contrast DES, 3-DES and AES?	Remember	CO2	ACS013.05
7.	Illustrate the procedure of key distribution in conventional encryption	Remember	CO2	ACS013.06
8.	Explain block cipher modes of operations.	Remember	CO2	ACS013.07
9.	Explain Diffie- Hellman algorithm.	Remember	CO2	ACS013.09
10.	Justify how DES algorithm uses feistel cipher structure?	Understand	CO2	ACS013.05
11.	Formulate AES encryption and decryption process with neat sketch?	Understand	CO2	ACS013.05
12.	Differentiate between AES and DES in a brief manner?	Understand	CO2	ACS013.05

13.	Demonstrate how the placement of encryption will works?	Remember	CO2	ACS013.06
14.	Explain briefly about RSA algorithm and ECC in a detail manner.	Understand	CO2	ACS013.09
15.	Explain all the principles of the public key crypto systems.	Remember	CO2	ACS013.06
16.	Explain how key is distributed in the RSA algorithm.	Understand	CO2	ACS013.10
17.	Explain briefly how diffusion and confusion increases complexity to thwart the cryptanalyst.	Remember	CO2	ACS013.06
18.	Explain elliptic curve cryptography.	Remember	CO2	ACS013.05
19.	Explain linear and differential cryptanalysis in a detail manner.	Understand	CO2	ACS013.05
20.	Differentiate Blowfish, AES and RC4?	Understand	CO2	ACS013.09
PART -C (CRITICAL THINKING QUESTIONS)				
1.	Show that in 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.	Remember	CO2	ACS013.05
2.	If a bit error occurs in the transmission of a cipher text character in 8-bit CFB mode how far does the error propagate?	Understand	CO2	ACS013.07
3.	Differentiate block cipher and stream cipher techniques?	Remember	CO2	ACS013.07
4.	Differentiate diffusion and confusion in the cryptography	Understand	CO2	ACS013.05
5.	Describe the differences between differential and linear cryptanalysis?	Remember	CO2	ACS013.05
6.	Explain why do some block cipher modes of operation only use encryption while others use both encryption and decryption.	Understand	CO2	ACS013.07
7.	Explain different types of stream ciphers with neat diagrams.	Remember	CO2	ACS013.08
8.	Describe why it is important to study the feistel cipher?	Remember	CO2	ACS013.05
9.	Explain briefly which parameters and design choices determine the actual algorithm of a feistel cipher.	Remember	CO2	ACS013.05
10.	Describe the purpose of the S-boxes in DES?	Understand	CO2	ACS013.05
UNIT – III				
PART - A (SHORT ANSWER QUESTIONS)				
1.	Explain Authentication requirements.	Understand	CO3	ACS013.11
2.	List authentication codes?	Understand	CO3	ACS013.11
3.	Explain Secure hash algorithm?	Understand	CO3	ACS013.13
4.	Discuss whirlpool.	Understand	CO3	ACS013.11
5.	Explain the steps in knapsack algorithm.	Understand	CO3	ACS013.13
6	Differentiate HMAC and CMAC?	Remember	CO3	ACS013.11
7.	List authentication requirements?	Understand	CO3	ACS013.11
8.	Differentiate MD4 and MD5?	Understand	CO3	ACS013.11
9.	Define HMAC.	Remember	CO3	ACS013.11
10.	Discuss CMAC.	Remember	CO3	ACS013.11
1.	Discuss Public – Key Infrastructure.	Understand	CO3	ACS013.14
2.	Mention key principles of Biometric Authentication?.	Remember	CO3	ACS013.14
3.	Differentiate between private and public key?	Understand	CO3	ACS013.14
4.	Enumerate uses of public key cryptography?	Understand	CO3	ACS013.14
5.	Define digital signatures.	Understand	CO3	ACS013.12
6.	Explain about X.509 certificate.	Remember	CO3	ACS013.14
7.	Differentiate simple and secure authentication dialogue in Kerberos	Remember	CO3	ACS013.12
8.	List X.509 services?	Understand	CO3	ACS013.14
9.	Define message digest?	Understand	CO3	ACS013.13
10.	List message authentication applications?	Understand	CO3	ACS013.11
PART -B (LONG ANSWER QUESTIONS)				
1.	Describe the following terms in detail a)whirlpool b)knapsack algorithm	Remember	CO3	ACS013.11
2.	Describe briefly what are the different kinds of the authentication requirements are there for message authentication?	Understand	CO3	ACS013.11
3.	Explain secure hash algorithms protocol.	Understand	CO3	ACS013.13
4.	Explain knapsack algorithm with an example.	Remember	CO3	ACS013.13
5	Explain whirlpool mechanism with an example.	Understand	CO3	ACS013.11
6.	Describe how hash algorithms will provide security?	Understand	CO3	ACS013.13

7.	Describe the differences between HMAC and CMAC?	Remember	CO3	ACS013.13
8.	Describe digital signatures with an example ?	Remember	CO3	ACS013.12
9.	Describe the different types of the message authentication codes and explain with an example?	Understand	CO3	ACS013.11
10.	Describe the message digest function in digital signatures and explain with an example?	Remember	CO3	ACS013.12
1.	Define biometric authentication and how it is important to support security n real time and suggest your answer?	Understand	CO3	ACS013.12
2.	Differentiate public key and private key and explain public key infrastructure with an example?	Understand	CO3	ACS013.14
3.	Define authentication service? Explain x.509 authentication services in a detail manner?	Understand	CO3	ACS013.14
4.	Describe the Kerberos security mechanism and explain why it is important in real time for providing security?	Remember	CO3	ACS013.13
5.	Differentiate Kerberos v4 and Kerberos v5?	Understand	CO3	ACS013.13
6.	Describe why Kerberos is more secure than the other security mechanisms?	Understand	CO3	ACS013.13
7.	List out management functions of PKIX and describe the process in public Key infrastructure?	Remember	CO3	ACS013.14
8	Discriminate how X.509 certificate is revoked?	Understand	CO3	ACS013.14
9	Describe the message digest function in digital signatures with an example?	Remember	CO3	ACS013.12
10.	Explain X.509 certificates with neat diagram.	Understand	CO3	ACS013.14
PART -C (CRITICAL THINKING QUESTIONS)				
1.	Describe what changes in HMAC are required in order to replace one underlying hash function with another?	Understand	CO3	ACS013.11
2.	Explain 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?	Understand	CO3	ACS013.11
3.	Describe what basic arithmetical and logical functions are used in MD5?	Remember	CO3	ACS013.13
4.	What is digital signature? Explain in detail.	Remember	CO3	ACS013.12
5.	Describe the differences between MD4 and MD5.specifically, to what extent? Do you think that MD5 is stronger than MD4, and why?	Understand	CO3	ACS013.13
6.	Explain what types of attacks are addressed by message authentication.	Understand	CO3	ACS013.11
7.	List some approaches to producing message authentication?	Remember	CO3	ACS013.11
8.	Describe what characters are needed in a secure hash function?	Remember	CO3	ACS013.13
9.	Describe public key infrastructure?	Remember	CO3	ACS013.14
10.	Explain SHA-1, show the values of W16,W17,W18,W19.	Understand	CO3	ACS013.13
11.	Explain digital signature and need of digital signature.	Remember	CO3	ACS013.12
UNIT – IV				
PART - A (SHORT ANSWER QUESTIONS)				
1.	What is PGP?	Remember	CO4	ACS013.15
2.	Explain why PGP is open source.	Understand	CO4	ACS013.15
3.	List out notations used in PGP?	Remember	CO4	ACS013.15
4.	List out services of PGP?	Remember	CO4	ACS013.15
5.	Explain e-mail compatibility.	Remember	CO4	ACS013.15
6.	Explain why does PGP generate a signature before Remembering.	Understand	CO4	ACS013.15
7.	Remember how does PGP provide public key management?	Understand	CO4	ACS013.15
8.	List MIME content types?	Remember	CO4	ACS013.15
9.	Write about IP Security.	Remember	CO4	ACS013.16
10.	Explain the utility of a detached signature.	Understand	CO4	ACS013.16
11.	Enumerate IP Security overview?	Understand	CO4	ACS013.16
12.	Define Authentication Header?	Remember	CO4	ACS013.16
13.	Explain encapsulating Security payload.	Remember	CO4	ACS013.16
14.	List Combining Security associations?	Understand	CO4	ACS013.16
15.	Discuss key management?	Understand	CO4	ACS013.16
16.	Define the over view of security?	Understand	CO4	ACS013.16

17.	Define key management?	Understand	CO4	ACS013.16
18.	What is header?	Understand	CO4	ACS013.16
19.	Write short note on IP security?	Understand	CO4	ACS013.16
20.	Describe the architecture of IP Security?	Understand	CO4	ACS013.16
PART -B (LONG ANSWER QUESTIONS)				
1.	Enumerate all services of PGP and explain with neat sketch?	Understand	CO4	ACS013.15
2.	Formulate on what basis Zimmermann has developed PGP for e-mail security?	Understand	CO4	ACS013.15
3.	Demonstrate the general format of PGP message with an example?	Understand	CO4	ACS013.15
4.	Generalize why in spite of symmetric key, public key and private key, uses three separate requirements what are those and explain why are used?	Understand	CO4	ACS013.15
5.	Demonstrate the general structure of Oakley key ?	Understand	CO4	ACS013.15
6.	Illustrate ISAKMP key management?	Understand	CO4	ACS013.15
7.	Justify why S/MIME is a security enhancement to MIME internet email format standard?	Understand	CO4	ACS013.15
8.	Explain of MIME specification with an example.	Understand	CO4	ACS013.15
9.	Demonstrate MIME transfer encoding techniques and certificate processing?	Understand	CO4	ACS013.15
10.	Illustrate S/MIME message?	Understand	CO4	ACS013.15
11.	Describe how encapsulating security payload is defined?	Understand	CO4	ACS013.16
12.	Demonstrate combining security associations?	Understand	CO4	ACS013.16
13.	Discuss about the key management in email security?	Understand	CO4	ACS013.15
14.	Discuss about the IP security architecture in detail?	Understand	CO4	ACS013.16
15.	Describe IP security overview?	Remember	CO4	ACS013.16
16.	Describe and explain how the security will be provided in Email?	Understand	CO4	ACS013.15
17.	Discuss the importance of the authentication header and explain its structure?	Remember	CO4	ACS013.16
18.	Define payload? And discuss about encapsulating security payload?	Remember	CO4	ACS013.16
19.	Discuss about the MIME content types?	Remember	CO4	ACS013.15
20.	Differentiate PGP and MIME types?	Understand	CO4	ACS013.15
PART -C (CRITICAL THINKING QUESTIONS)				
1.	Explain why PGP generate a signature before remembering	Understand	CO4	ACS013.15
2.	Explain why is R64 conversion is useful for an e-mail application.	Understand	CO4	ACS013.15
3.	Describe the differences between MIME and S/MIME?	Understand	CO4	ACS013.15
4.	Explain the examples of applications of IPSec?	Remember	CO4	ACS013.16
5.	Define what are the services provided by IPSec?	Understand	CO4	ACS013.16
6.	Describe what are the basic approaches to bundling SAs?	Understand	CO4	ACS013.16
7.	Explain why is the segmentation and reassembly function in PGP	Remember	CO4	ACS013.15
8.	Define what parameters to identify an SA and what parameters characterize the nature of particular SA?	Understand	CO4	ACS013.16
9.	Describe and support your answer how PGP use the concept of trust?	Understand	CO4	ACS013.15
10.	Explain why does ESP include a padding field?	Remember	CO4	ACS013.16
UNIT – V				
PART - A (SHORT ANSWER QUESTIONS)				
1.	Collaborate different file access activities used for intrusion detection?	Understand	CO5	ACS013.18
2.	Enumerate types of viruses?	Understand	CO5	ACS013.19
3.	Remember how does a worm propagate?	Understand	CO5	ACS013.19
4.	Remember how biometrics used instead of password for authentication?	Understand	CO5	ACS013.20
5.	Discriminate three benefits that can be provided by an intrusion	Understand	CO5	ACS013.18
6.	Differentiate statistical anomaly detection and rule based intrusion	Understand	CO5	ACS013.18
7.	Explain firewall and principles of firewall?	Remember	CO5	ACS013.20
8.	List files access activities used for intrusion detection?	Remember	CO5	ACS013.18
9.	Demonstrate techniques used to avoid guessable password?	Remember	CO5	ACS013.20
10.	List out design goals for a firewall?	Understand	CO5	ACS013.20
11.	Demonstrate an application-level gateway?	Understand	CO5	ACS013.20
12.	Discuss in the context of access control ?	Remember	CO5	ACS013.17
13.	Evaluate hoe firewall is different from intrusion detection system?	Remember	CO5	ACS013.20
14.	Differentiate packet filter routing and a state full inspection firewall?	Understand	CO5	ACS013.20

15.	Remember how biometrics used instead of password for authentication?	Understand	CO5	ACS013.20
16.	Explain protocols that comprise SSL.	Understand	CO5	ACS013.17
17.	State alert codes of TLS protocol?	Understand	CO5	ACS013.17
18.	State parameters that define SSL session state?	Understand	CO5	ACS013.17
19.	Differentiate SSL and TLS protocols?	Understand	CO5	ACS013.17
20.	Explain services provided by SSL record protocol.	Understand	CO5	ACS013.17
PART -B (LONG ANSWER QUESTIONS)				
1.	Demonstrate 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?	Remember	CO5	ACS013.18
2.	Describe how hackers exploit vulnerabilities in the network-based computing systems?	Understand	CO5	ACS013.18
3.	Analyze various approaches to prevention and detection from users?	Understand	CO5	ACS013.18
4.	Remember software threats to systems with a special emphasis on viruses and worms?	Understand	CO5	ACS013.19
5.	Enumerate counter measure for viruses and worms?	Understand	CO5	ACS013.19
6.	Describe the different types of the secure electronic transaction	Understand	CO5	ACS013.18
7.	Explain different types of the viruses and firewalls in web security?	Understand	CO5	ACS013.20
8.	Explain the concept of the virtual electronics?	Understand	CO5	ACS013.20
9.	Describe the firewall design principles in a detail manner?	Remember	CO5	ACS013.20
10.	Discuss about the cross site scripting vulnerability?	Understand	CO5	ACS013.18
11.	Define transaction? And explain the inter branch payment transactions?	Remember	CO5	ACS013.17
12.	Discuss the different types of firewalls in a detail manner?	Understand	CO5	ACS013.20
13.	Differentiate socket layer security and transport security ?	Understand	CO5	ACS013.17
14.	Define term intruders? Discuss about intrusion detection password management?	Remember	CO5	ACS013.18
15.	Define threat and attacks? And describe virus and related threats?	Remember	CO5	ACS013.19
16.	Discuss standard approach to the protection of local computer assets external threats?	Understand	CO5	ACS013.19
17.	Discuss firewall design principles and also explain techniques?	Understand	CO5	ACS013.20
18.	Discuss how intrusion prevention is achieved through password management?	Understand	CO5	ACS013.18
19.	Justify Intrusion provides early warning of an intrusion so that action can be taken to prevent or minimize damage?	Understand	CO5	ACS013.18
20.	Differentiate statistical anomaly detection and rule–based intrusion detection?	Understand	CO5	ACS013.18
PART -C (CRITICAL THINKING QUESTIONS)				
1.	Briefly define the principal categories of SET participants?	Remember	CO5	ACS013.17
2.	Briefly define the parameters that define an SSL session state?	Remember	CO5	ACS013.17
3.	In SSL and TLS, why is there a separate change cipher Spec protocol rather than including a change cipher-Spec message in the Handshake protocol?	Understand	CO5	ACS013.17
4.	Describe what is dual signature and what is its purpose?	Understand	CO5	ACS013.17
5.	Briefly define three classes of intruders?	Remember	CO5	ACS013.18
6.	Describe what are the two common techniques used to protect a password file?	Understand	CO5	ACS013.20
7.	Define firewall? Explain the design principles in detail?	Remember	CO5	ACS013.20
8.	Explain briefly about the secure inter branch transactions?	Understand	CO5	ACS013.17
9.	Describe about the cross sire scripting vulnerability?	Understand	CO5	ACS013.19
10.	Explain briefly about the virtual elections?	Understand	CO5	ACS013.17

Prepared By:

Ms B Geetavani, Assistant Professor

HOD, IT