INSTITUTE OF AERONAUTICAL ENGINEERING
(Autonomous)

INFORMATION TECHNOLOGY

TUTORIAL QUESTION BANK

Course Title	**INFORMATION SECURITY**			
Course Code	**A70522**			
Regulation	**R15 - JNTUH**			
Course Structure	Lectures	Tutorials	Practicals	Credits
	4	-	-	4
Course Coordinator	Dr. P L Srinivasa Murthy Professor			
Team of Instructors	Dr. P L Srinivasa Murthy Professor			

OBJECTIVES:

To meet the challenge of ensuring excellence in engineering education, the issue of quality needs to be addressed, debated and taken forward in a systematic manner. Accreditation is the principal means of quality assurance in higher education. The major emphasis of accreditation process is to measure the outcomes of the program that is being accredited.

In line with this, Faculty of Institute of Aeronautical Engineering, Hyderabad has taken a lead in incorporating philosophy of outcome based education in the process of problem solving and career development. So, all students of the institute should Understand the depth and approach of course to be taught through this question bank, which will enhance learner’s learning process.

S. No.	Questions	Blooms Taxonomy Level	Course Outcomes
UNIT – I			
Part-A(Short Answer Questions)			
1	Explain security attacks?	Understand	1
2	Enumerate traffic analysis?	Remember	1
3	Categorize active attacks?	Remember	1
4	Categorize passive attacks?	Understand	4
5	Mention the key principles of security?	Understand	4
6	Distinguish active and passive attacks?	Understand	1
7	Enumerate the mechanisms implemented for confidentiality?	Remember	1
8	List briefly categories of security mechanisms?	Remember	1
9	Specify basic tasks for defining a security services?	Remember	2
10	Differentiate symmetric and asymmetric encryption?	Remember	1
11	Define cryptanalysis?	Remember	1
12	Explain Security approaches?	Understand	1
13	Specify model for Network Security?	Remember	1
14	Explain the need for security?	Understand	1
15	Distinguish substitution techniques?	Understand	1
16	Distinguish transposition techniques?	Understand	1
17	Differentiate encryption and decryption?	Understand	2
18	Differentiate symmetric and asymmetric key cryptography?	Remember	1
19	Define steganography?	Remember	1

20	Enumerate key range **and key size?**	Remember	2
Part-B(Long Answer Questions)			
1.	Describe the following Security attacks Security services Security mechanisms	Remember	2
2.	Define cryptanalysis. Mention the types of cryptanalysis and in detail theamount of information known to cryptanalytic?	Remember	1,2
3.	Demonstrate model for internetwork security with neat diagram?	Understand	1,2
	Demonstrate how internet standards have been standardized by using RFC?	Understand	1,2
4.	Differentiate TCP and UDP session hijacking?	Remember	1,2
5.	Define Caesar cipher? And calculate the encryption and decryption for he following plain text P=”COME TO MY HOME” by using caser cipher with Key k=3?	Understand	1,2
6.	Convert the following plain text message P=”THIS IS NOT A GOLD” into cipher text with key k=”play fair example” by using play fair cipher technique?	Understand	1,2
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	1,2
8.	Convert the following plain text P=”COME NOW” into cipher text by using one-time pad cipher(Vernam cipher) with key K=”NCBTZQARX”	Understand	1,2
9.	Convert 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	1,2
10.	Understand and contrast all kinds of cipher techniques in the cryptography?	Understand	1,2
11.	Convert the following plain text message P=”I AM NOT A KID TO DO THAT THINGS “ into cipher text by using mono alphabetic cipher technique	Understand	1,2
12.	Convert the following plain text message P=”WE ARE IARE CSE STUDENTS” into cipher text with key K=”deceptive” with key epetition	Understand	
13.	Convert the following plain text message P=”come to my home today	Understand	1,2
Part-C(Problem solving and 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?	Remember	1,2
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	1,2
3	Convert the following plain text P=”Help me” into cipher text by usingHill cipher with key K=which is a 2X2 matrix(only encryption)	Understand	1,2
4	Convert the following plain text P=”Come Today” into cipher text by using one-time pad cipher(Vernam cipher) with key K=”NCBTZQARX”	Understand	1,2
5	Convert the following plain text message P=0110111 into cipher text by using one-time pad cipher with key K=1011001.calculate both encryption and decryption for the above message.	Understand	1,2
6	Understand and contrast all kinds of cipher techniques in the cryptography?	Understand	1,2
7	Convert the following plain text message P=”I discovered a gravitational force “ into cipher text by using mono alphabetic cipher technique	Understand	1,2

8	Convert the following plain text message P=”we are discovered save yourself” into cipher text with key K=”deceptive” with key repetition	Understand	1,2
9	Convert the following plain text message P=”come to my home tomorrow” into cipher text message by using the Rail fence technique	Understand	1,2
10	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	1,2
UNIT – II			
Part-A(Short Answer Questions)			
1	Understand stream and block ciphers with examples?	Understand	2
2	Differentiate DES, AES, Blowfish algorithms?	Understand	2
3	Differentiate Differential and Linear Cryptanalysis,	Remember	2
4	Enumerate design parameters of feistel cipher structure?	Remember	2
5	Define product cipher?	Remember	2
6	Lists block cipher modes of operation?	Remember	2
7	Explain essential ingredients of symmetric cipher?	Understand	2
8	Differentiate link and end-to-end encryption?	Remember	2
9	Differentiate session key and master key?	Remember	2
10	State advantages of counter mode?	Understand	2
11	Specify the design criteria of block cipher?	Understand	2
12	Explain RC4 Location?	Understand	2
13	Enumerate placement of encryption function?	Remember	2
14	List key distribution Asymmetric key Ciphers?	Remember	3
15	Explain principles of public key cryptosystems?	Understand	3
16	Differentiate RSA Diffie-Helman, ECC Key Distribution Algorithm?	Remember	3
17	Explain the procedure for DES algorithm?	Understand	3
18	List the steps in AES algorithms?	Remember	4
19	Explain the procedure for RSA algorithm?	Understand	3
20	List the steps in ECC Key Distribution algorithm?	Remember	3
Part-B(Long Answer Questions)			
1	Describe how Compile the process how RC4 decryption is reverse of its encryption?	Understand	3
2	Justify how DES algorithm uses feistel cipher structure?	Understand	3
3	Enumerate the principles of conventional encryption algorithms?	Remember	3
4	Demonstrate how encryption is misused to attack the system?	Understand	3
5	Recite round function evaluation in feistel cipher structure?	Remember	3
6	Understand and contrast DES, 3-DES and AES?	Understand	3
7	Illustrate the procedure of key distribution in conventional encryption	Remember	3
8	Illustrate how secure hash function is alternative to MAC?	Remember	4
9	Enumerate the different steps of SHA to generate message digest?	Remember	4
10	Justify how DES algorithm uses feistel cipher structure?	Understand	3

10	Formulate AES encryption and decryption process with neat sketch?	Understand	3,4
11	Differentiate between AES and DES in a brief manner?	Understand	3,4
12	Demonstrate how the placement of encryption will works?	Understand	4
13	Explain briefly about RSA algorithm and ECC in a detail manner?	Understand	4
14	Explain all the principles of the public key crypto systems?	Understand	3,4
15	Explain how key is distributed in the RSA algorithm?	Understand	3,4
16	Explain briefly how diffusion and confusion increases complexity to hwart the cryptanalyst?	Understand	3
17	Explain linear and differential cryptanalysis in a detail manner?	Understand	4
18	Demonstrate how SSL provide security services between TCP application	Understand	4
19	Remember how SSL provide confidentiality using symmetric encryption and decryption?	Remember	3,4
20	Remember how TLS provide confidentiality using symmetric encryption and decryption?	Remember	3,4

Part-C(Problem solving and 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	3
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?	Remember	3
3	Differentiate block cipher and stream cipher techniques?	Understand	3
4	Differentiate diffusion and confusion in the cryptography?	Understand	3,4
5	Describe why it is important to study the feistel cipher?	Remember	3,4
6	Explain briefly which parameters and design choices determine the actual algorithm of a feistel cipher?	Understand	4
7	Describe the purpose of the S-boxes in DES?	Remember	3
8	Describe the differences between differential and linear cryptanalysis?	Remember	4
9	Explain why do some block cipher modes of operation only use encryption while others use both encryption and decryption?	Understand	3,4

UNIT – III

Part-A(Short Answer Questions)

1	Explain Authentication requirements?	Understand	5
2	List authentication codes?	Remember	5
3	Explain Secure hash algorithm?	Understand	5
4	Discuss whirlpool?	Understand	5
5	Differentiate HMAC and CMAC?	Remember	5
6	Explain the steps in knapsack algorithm?	Understand	6
7	Discuss Public – Key Infrastructure?	Remember	6
8	Mention key principles of Biometric Authentication?.	Remember	5
9	Differentiate between private and public key?	Remember	6
10	Enumerate uses of public key cryptography?	Remember	6
11	Differentiate public key and conventional encryption?	Remember	6
12	Explain the rules of public and private key?	Understand	6
13	Explain the principles elements of a public key cryptography?	Remember	6
14	Specify the application of public key cryptography?	Understand	6
15	List four general characteristics of a scheme for distribution of the	Remember	5
16	Discuss about key management in public key cryptography?	Remember	5
17	Define digital signatures?	Remember	5
18	Explain about X.509 certificate?	Remember	5
19	List the disadvantages of Diffie-Helman key exchange algorithm?	Understand	5
20	Differentiate simple and secure authentication dialogue in Kerberos	Remember	5

Part-B(Long Answer Questions)

1	Define biometric authentication and how it is important to support security n real time and suggest your answer?	Understand	5
2	Differentiate public key and private key and explain public key infrastructure with an example?	Remember	5

3	Define authentication service? And explain x.509 authentication services in a detail manner?	Understand	5
4	Describe the Kerberos security mechanism and explain why it is important n real time for providing security?	Remember	6
5	Describe the following terms in detail a)whirlpool b)knapsack algorithm	Understand	5,6
6	Differentiate Kerberos v4 and Kerberos v5?	Remember	6
7	List out management functions of PKIX and describe the process in	Remember	6
8	Discriminate how X.509 certificate is revoked?	Remember	6
9	Demonstrate use of realm and justify the usage? Invent the context of	Understand	6
10	Illustrate approaches to secure user authentication in a distributed	Remember	6
11	Explain with an neat example how knapsack algorithm will works and	Remember	
12	Explain whirlpool mechanism with an example?	Understand	6
13	Describe briefly what are the different kinds of the authentication requirements are there for message authentication?	Understand	6
14	Describe how hash algorithms will provide security?	Understand	6
15	Describe the differences between HMAC and CMAC?	Remember	6
16	Describe digital signatures with an example ?	Understand	6
17	Explain biometric authentication with an example?	Understand	6
18	Describe why Kerberos is more secure than the other security mechanisms?	Understand	6
19	Describe the different types of the message authentication codes and explain with an example?	Remember	6
20	Describe the message digest function in digital signatures and explain with an example?	Understand	6

Part-C(Problem solving and critical thinking questions)

1	Describe the differences between big-endian format and little- endian format?	Remember	5
2	Explain SHA-1, show the values of W16,W17,W18,W19.	Understand	5,6
3	Describe what changes in HMAC are required in order to replace one underlying hash function with another?	Remember	5
4	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	5,6
5	Describe what basic arithmetical and logical functions are used in MD5?	Remember	5
6	Describe what basic arithmetical and logical functions are used in RIPEMD-160?	Remember	5,6
7	Describe the differences between MD$ and MD5.specifically, to what extent t\do you think that MD5 is stronger than MD4, and why?	Remember	5
8	Explain what types of attacks are addressed by message authentication?	Understand	5,6
9	List some approaches to producing message authentication?	Remember	5,6
10	Describe what characters are needed in a secure hash function?	Remember	5

UNIT – IV

Part-A(Short Answer Questions)

1	Define PGP?	Remember	5
2	Explain why PGP is open source?	Understand	5
3	List out notations used in PGP?	Remember	5
4	List out services of PGP?	Remember	5
5	Explain e-mail compatibility?	Understand	5
6	Explain why does PGP generate a signature before Remembering	Understand	5
7	Remember how does PGP provide public key management?	Remember	5
8	List MIME content types?	Remember	5
9	Explain S/MIME IP Security ?	Understand	6
10	Explain the utility of a detached signature?	Understand	6
11	Enumerate IP Security overview?	Remember	6
12	Define Authentication Header?	Remember	6

13	Explain encapsulating Security payload?	Understand	6
14	List Combining Security associations?	Remember	5,6
15	Discuss key management?	Remember	5,6
16	Define the over view of security?	Remember	5,6
17	Define key management?	Remember	5,6
18	Define header?	Remember	5,6
19	Define IP security?	Remember	5,6
20	Describe the architecture of IP Security?	Remember	5,6
	Part-B(Long Answer Questions)		
1	Formulate on what basis Zimmermann has developed PGP for e-mail security?	Understand	5 5
2	Enumerate all services of PGP and explain with neat sketch	Remember	5
3	Generalize why inspite of symmetric key, public key and private key, uses three separate requirements what are those and explain why are used?	Understand	5
4	Demonstrate the general format of PGP message with an example?	Understand	5
5	Demonstrate the general structure of private key ring?	Understand	5
6	Illustrate different approaches to public key management?	Remember	5
7	Justify why S/MIME is a security enhancement to MIME internet email format standard?	Remember	5
8	Explain of MIME specification with an example?	Understand	5
9	Demonstrate MIME transfer encoding techniques and certificate processing?	Understand	5
10	Illustrate S/MIME message?	Remember	5
11	Describe how encapsulating security payload is defined?	Understand	5
12	Demonstrate combining security associations?	Understand	5
13	Discuss about the key management in email security?	Understand	5,6
14	Discuss about the IP security architecture in detail?	Understand	5,6
15	Describe IP security overview?	Understand	5,6
16	Describe and explain how the security will be provided in Email?	Understand	5,6
17	Discuss the importance of the authentication header and explain its structure?	Understand	5,6
18	Define payload? And discuss about encapsulating security payload?	Understand	5,6
19	Discuss about the MIME content types?	Understand	5,6
20	Differentiate PGP and MIME types ?	Understand	5,6
	Part-C(Problem solving and critical thinking questions)		
1	Explain why does PGP generate a signature before Remembering compression?	Understand	5
2	Explain why is the segmentation and reassembly function in PGP needed?	Understand	5
3	Explain why is R64 conversion is useful for an e-mail application?	Understand	5
4	Describe the differences between MIME and S/MIME?	Remember	5
5	Describe and support your answer how PGP use the concept of trust?	Remember	5
6	Define what parameters to identify an SA and what parameters characterize the nature of particular SA?	Remember	5,6
7	Explain why does ESP include a padding field?	Understand	5,6
8	Describe what are the basic approaches to bundling SAs?	Remember	5,6
9	Explain the examples of applications of IPSec?	Understand	5,6
10	Define what are the services provided by IPSec?	Remember	5,6
	UNIT – V		
	Part-A(Short Answer Questions)		
1	Collaborate different file access activities used for intrusion detection?	Understand	6
2	Enumerate types of viruses?	Remember	6
3	Remember how does a worm propagate?	Understand	6
4	Remember how biometrics used instead of password for authentication?	Remember	6

5	Discriminate three benefits that can be provided by an intrusion	Remember	6
6	Differentiate statistical anomaly detection and rule based intrusion	Remember	6
7	List files access activities used for intrusion detection?	Remember	6
8	Demonstrate techniques used to avoid guessable password?	Understand	6
9	List out design goals for a firewall?	Remember	6
10	Demonstrate an application-level gateway?	Understand	6
11	Discuss in the context of access control, what is the difference between	Understand	7
12	Evaluate hoe firewall is different from intrusion detection system?	Remember	7
13	Differentiate packet filter routing and a state full inspection firewall?	Remember	7
14	Remember how biometrics used instead of password for authentication?	Remember	7
15	Explain protocols that comprise SSL?	Understand	7
16	State alert codes of TLS protocol?	Remember	7
17	State parameters that define SSL session state?	Remember	7
19	Differentiate SSL and TLS protocols?	Understand	7
20	Explain services provided by SSL record protocol?	Understand	7
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 thispacket be read and analyzed?	Understand	6,7
2	Describe how hackers exploit vulnerabilities in the network-based computing systems?	Remember	6,7
3	Analyze various approaches to prevention and detection from users?	Remember	6,7
4	Remember software threats to systems with a special emphasis on virusesand worms?	Remember	6,7
5	Enumerate counter measure for viruses and worms?	Remember	6,7
6	Describe the different types of the secure electronic transaction intruders?	Understand	6,7
7	Explain different types of the viruses and firewalls in web security?	Understand	6,7
8	Explain the concept of the virtual electronics?	Understand	6,7
9	Describe the firewall design principles in a detail manner?	Understand	6,7
10	Discuss about the cross site scripting vulnerability?	Understand	6,7
11	Define transaction? And explain the inter branch payment transactions?	Understand	7
12	Discuss the different types of firewalls in a detail manner?	Understand	7
13	Differentiate socket layer security and transport security ?	Understand	7
14	Define term intruders? Discuss about intrusion detection password management?	Understand	7
15	Define threat and attacks? And describe virus and related threats?	Understand	7
16	Discuss standard approach to the protection of local computer assets external threats?	Understand	7
17	Discuss firewall design principles and also explain techniques?	Understand	7
18	Discuss how intrusion prevention is achieved through password management?	Understand	7
19	Justify Intrusion provides early warning of an intrusion so that action can be taken to prevent or minimize damage?	Understand	7
20	Differentiate statistical anomaly detection and rule–based intrusion detection?	Remember	7
Part-C(Problem solving and critical thinking questions)			
1	Briefly define the principal categories of SET participants?	Remember	7
2	Briefly define the parameters that define an SSL session state?	Remember	7
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	7

4	Describe what is dual signature and what is its purpose?	Remember	7
5	Briefly define three classes of intruders?	Remember	7
6	Describe what are the two common techniques used to protect a password file?	Remember	7
7	Define firewall? And explain the design principles in detail?	Remember	7
8	Explain briefly about the secure inter branch transactions?	Understand	7
9	Describe about the cross sire scripting vulnerability?	Remember	7
10	Explain briefly about the virtual elections?	Understand	7

Prepared By: Dr. P L Srinivasa Murthy, Professor

HOD, IT