



# INSTITUTE OF AERONAUTICAL ENGINEERING (Autonomous)

Dundigal, Hyderabad - 500 043

## INFORMATION TECHNOLOGY

### ASSIGNMENT QUESTIONS

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

#### ASSIGNMENT-I

S. No.	Question	Blooms Taxonomy Level	Course Outcomes
<b>UNIT – I</b>			
1	Describe the following Security attacks Security services Security mechanisms	Remember	1,2
2	Define cryptanalysis. Mention the types of cryptanalysis and in detail the amount of information known to cryptanalytic?	Remember	1,2
3	Demonstrate model for internetwork security with neat diagram?	Understand	1,2
4	Demonstrate how internet standards have been standardized by using RFC?	Understand	1,2
5	Enumerate man in-middle attack in network?	Remember	2
6	Discriminate how buffer overflow is categorized under software weakness?	Remember	2
7	Demonstrate ARP attack in the network with an example?	Understand	2
8	Enumerate the security goals and explain each with an example?	Remember	2
9	Understand and contrast active and passive attacks?	Understand	2
10	Explain essential ingredients of symmetric cipher?	Understand	1,2
11	Differentiate link and end-to-end encryption?	Understand	1,2
12	Differentiate session key and master key?	Understand	1,2
13	State advantages of counter mode?	Remember	1,2
14	Recite round function evaluation in feistel cipher structure?	Understand	1,2

<b>UNIT – II</b>			
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?	Remember	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	Understand	3
8	Illustrate how secure hash function is alternative to MAC?	Understand	4
9	Enumerate the different steps of SHA to generate message digest?	Remember	4
10	Formulate AES encryption and decryption process with neat sketch?	Understand	3,4
11	Demonstrate how SSL provide security services between TCP application	Understand	11
12	Remember how SSL provide confidentiality using symmetric encryption	Remember	11
13	Remember how TLS provide confidentiality using symmetric encryption	Remember	11
14	List four general characteristics of a scheme for distribution of the public	Remember	3
15	Discuss about key management in public key cryptography?	Understand	3
16	Discuss digital signatures?	Understand	3
17	Differentiate simple and secure authentication dialogue in Kerberos v4?	Understand	4
18	List out management functions of PKIX and describe the process in detail?	Remember	3,4
<b>UNIT – III</b>			
1	Discriminate the requirements that must be fulfilled by public key	Remember	5
2	Assess how to debug the RSA encryption algorithm?	Remember	5
3	Demonstrate RSA public key encryption algorithm?	Understand	5
4	Describe the following	Remember	6
5	Compile how public keys are been certified in RSA and Diffie Hellman	Understand	5,6
6	Differentiate Kerberos v4 and Kerberos v5?	Understand	6
7	List out management functions of PKIX and describe the process in detail?	Remember	6
8	Discriminate how X.509 certificate is revoked?	Remember	6
<b>ASSIGNMENT-II</b>			
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	Understand	6
11	Understand and contrast DES, 3-DES and AES?	Understand	2
12	Illustrate the procedure of key distribution in conventional encryption	Understand	2
13	Discuss the security implications of following centralization?	Understand	2
14	Enumerate the different steps of SHA to generate message digest?	Remember	2
15	Formulate AES encryption and decryption process with neat sketch?	Understand	2
<b>UNIT – IV</b>			
1	Formulate on what basis Zimmermann has developed PGP for e-mail security?	Understand	7
2	Enumerate all services of PGP and explain with neat sketch	Remember	7
3	Generalize why inspite of symmetric key, public key and private key, PGP uses three separate requirements what are those and explain why are they used?	Understand	7
4	Demonstrate the general format of PGP message with an example?	Understand	7
5	Demonstrate the general structure of private key ring?	Understand	7
6	Illustrate different approaches to public key management?	Understand	7
7	Justify why S/MIME is a security enhancement to MIME internet e-mail format standard?	Remember	8
8	Explain of MIME specification with an example?	Understand	8
9	Demonstrate MIME transfer encoding techniques and certificate processing?	Understand	8
10	Illustrate S/MIME message?	Understand	8

UNIT – V			
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?	Understand	15
2.	Describe how hackers exploit vulnerabilities in the network-based computing systems?	Remember	15,16
3.	Analyze various approaches to prevention and detection from unauthorized users?	Understand	15,16
4.	Remember software threats to systems with a special emphasis on viruses and worms?	Remember	15,16
5.	Enumerate counter measure for viruses and worms?	Remember	15,16
6.	Discuss standard approach to the protection of local computer assets from external threats?	Understand	15,16
7.	Discuss firewall design principles and also explain techniques?	Understand	15,16
8.	Discuss how intrusion prevention is achieved through password management?	Understand	15,16
9.	Justify Intrusion provides early warning of an intrusion so that defensive action can be taken to prevent or minimize damage?	Understand	15,16
10.	Differentiate statistical anomaly detection and rule-based intrusion detection?	Understand	15,16

Prepared By: Dr. P L Srinivasa Murthy, Professor

HOD, IT