Hall Ticket No | | | | | | | | | | | Question Paper Code:ACS013

INSTITUTE OF AERONAUTICAL ENGINEERING

(Autonomous)

Dundigal, Hyderabad - 500 043

MODEL QUESTION PAPER

Four B.Tech VIII Semester End Examinations, May – 2020

Regulations: IARE - R16

INFORMATION SECURITY

[CSE/IT]

Time:3Hours **Max Marks:70**

Answer ONE Question from each Unit
All Questions Carry Equal Marks
All parts of the question must be answered in one place only

UNIT-I

1	a.	Explain security attacks, security services and security mechanisms with neat diagrams.	7M
	b.	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?	7M
2.	a.	Explain Caesar cipher and mono-alphabetic ciphers with examples?	7M
	b.	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?	7M

UNIT-II

3	a.	Explain the Advanced Encryption Standard algorithm. Write the difference between DES and AES.	7M
	b.	Explain briefly which parameters and design choices determine the actual algorithm of a feistel cipher.	7M
4	a.	Explain why do some block cipher modes of operation only use encryption while others use both encryption and decryption.	7M
	b.	Explain linear and differential cryptanalysis in a detail manner.	7M

UNIT-III

5	a.	Describe briefly what are the different kinds of the authentication requirements are there for message authentication?	7M
	b.	Describe the message digest function in digital signatures and explain with an example?	7M
6	a.	Describe the Kerberos security mechanism and explain why it is important in real time for providing security?	7M
	b.	Explain the message digest function in digital signatures with an example?	7M

UNIT-IV

7	a.	What is PGP? Discuss in detail about Pretty Good Privacy with example.	7M
	b.	Generalize why in spite of symmetric key, public key and private key, uses three separate requirements what are those and explain why are used?	7M
8	a.	Define S/MIME? Explain in detail about the importance of S/MIME in E-mail security.	7M
	b.	Define what parameters to identify an SA and what parameters characterize the nature of particular SA?	7M

UNIT-V

9	a.	What is Intrusion? Discuss Intrusion detection system with neat diagram? Explain the need of Intrusion detection.	7M
	b.	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 analysed?	7M
10	a.	Define term intruders? Discuss about intrusion detection password management?	7M
	b.	Discuss how intrusion prevention is achieved through password management?	7M

COURSE OBJECTIVIES:

The course should enable the students to:

I	Learn the basic categories of threats to computers and networks
II	Understand various cryptographic algorithms and be familiar with public-key cryptography.
III	Apply authentication functions for providing effective security.
IV	Analyze the application protocols to provide web security.
V	Discuss the place of ethics in the information security area.

COURSE OUTCOMES:

CO1	Understand the basic Concepts of attacks on computer, computer security.
CO2	Understand the concepts of symmetric key ciphers.
CO3	Describe 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 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 private and public key in encryption and decryption 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 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	Understand various types of viruses and its vulnerabilities.
ACS013.20	Describe various types of firewalls and analyze the security levels of these.

MAPPING OF SEMESTER END EXAMINATION TO COURSE LEARNING OUTCOMES:

SEE Question No.		Course Learning Outcomes		Course Outcomes	Blooms Taxonomy Level
1	a	ACS013.02	Explain various substitution techniques such as play-fair cipher, mono-alphabetic cipher and hill cipher.	CO1	Understand
	b	ACS013.01	Understand the different types of attacks, security mechanisms, security services.	CO1	Remember
2	a	ACS013.01	Understand the different types of attacks, security mechanisms, security services.	CO1	Understand
	b	ACS013.03	Understand various Transposition techniques such as row transposition and rail-fence.	CO1	Remember
3	a	ACS013.05	Apply the symmetric algorithm for message transmission and analyze the security level of it..	CO2	Understand
	b	ACS013.06	Understand various asymmetric key encryption algorithms for message encryption and decryption.	CO2	Understand
4	a	ACS013.05	Apply the symmetric algorithm for message transmission and analyze the security level of it..	CO2	Understand
	b	ACS013.06	Understand various asymmetric key encryption algorithms for message encryption and decryption.	CO2	Understand
5	a	ACS013.11	Explain the role of the message authentication in message transmission.	CO3	Understand
	b	ACS013.13	Explain and demonstrate the role of different types of hash functions for providing security.	CO3	Remember
6	a	ACS013.11	Explain the role of the message authentication in message transmission.	CO3	Understand
	b	ACS013.11	Explain the role of the message authentication in message transmission.	CO3	Understand
7	a	ACS013.15	Explain S/MIME and PGP for transmitting mail from sender to receiver.	CO4	Remember
	b	ACS013.16	Explain IP security for internet protocol and analyze how it provides security.	CO4	Remember
8	a	ACS013.15	Explain S/MIME and PGP for transmitting mail from sender to receiver.	CO4	Remember
	b	ACS013.16	Explain IP security for internet protocol and analyze how it provides security.	CO4	Remember
9	a	ACS013.18	Analyze various types of intrusion detection techniques.	CO5	Understand
	b	ACS013.17	Describe the security socket layer and transport layer security for web security.	CO5	Understand
10	a	ACS013.20	Describe various types of firewalls and analyze the security level of these.	CO5	Understand
	b	ACS013.17	Describe the security socket layer and transport layer security for web security.	CO5	Understand

Signature of the faculty **HOD, IT**