

**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. Consider the plaintext: “PROTOCOL” Secret key: “NETWORK” What is the corresponding cipher text using play fair cipher method. 7M
- b. Define security and explain the need of security? 7M
2. a. Explain the model of network security. What is the need of the model of network security? 7M
- b. Define steganography? Explain different types of steganography with suitable examples? 7M

**UNIT-II**

- 3 a. Explain the Advanced Encryption Standard algorithm. Write the difference between DES and AES. 7M
- b. What is blowfish algorithm? Consider a Diffie-Hellman scheme with a common prime  $q=11$ , and a primitive root  $\alpha=2$ . 7M
- 4 a. Explain Data Encryption Standard encryption and decryption process with suitable examples. 7M
- b. Discuss Elliptic Curve Cryptography algorithm with a neat diagram. Explain the need of ECC. 7M

**UNIT-III**

- 5 a. What is meant by authentication? Explain the HMAC authentication algorithm with authentication codes? 7M
- b. Explain the need of hash function. Discuss the knapsack algorithm and needs of knapsack algorithm. 7M

- 6 a. List out the different types of authentication applications. Explain different types of Kerberos? 7M  
b. Explain the biometric authentication and the need of the biometric authentication in real world. 7M

#### UNIT-IV

- 7 a. What is PGP? Discuss in detail about Pretty Good Privacy with example. 7M  
b. Mention IP Security architecture with a neat diagram and explain the importance of IP Security. 7M
- 8 a. Define S/MIME? Explain in detail about the importance of S/MIME in E-mail security. 7M  
b. Discuss in detail about encapsulating security payload with a neat diagram and explain the uses of it. 7M

#### UNIT-V

- 9 a. What is Intrusion? Discuss Intrusion detection system with neat diagram? Explain the need of Intrusion detection. 7M  
b. Explain the Secure Socket Layer with neat diagrams. Discuss the need of Secure Socket Layer? 7M
- 10 a. Write a short note on firewall design principles and discuss the various types of firewalls? 7M  
b. Discuss in detail about secure electronic transaction? Explain the need of secure electronic transaction. 7M



# INSTITUTE OF AERONAUTICAL ENGINEERING (Autonomous)

## **COURSE OBJECTIVES:**

**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:**

<b>S. No</b> <b>Course Learning Outcomes</b>	
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 faculty**

**HOD, CSE**