17/6/23 - FN.

Reg. No. : | | | | | | | | | | | | |

Question Paper Code : 50056

B.E./B.Tech. DEGREE EXAMINATIONS, APRIL/MAY 2023.

Sixth Semester

Artificial Intelligence and Data Science

AD 8602 – DATA AND INFORMATION SECURITY

(Regulations 2017)

Time : Three hours Maximum : 100 marks

Answer ALL questions.

PART A — (10 × 2 = 20 marks)

1. How CIA triad is important in computer security?

2. Differentiate between modular arithmetic and ordinary arithmetic.

3. Why do some block cipher modes of operation only use encryption while others use both encryption and decryption?

4. In the context of a hash function, what is a compression function?

5. Compare between password based authentication and token based authentication.

6. How do most current X.509 implementations check the validity of signatures on a certificate?

7. Compare between the implementations of the discretionary access control models on Unix and Linux systems and those on Windows systems.

8. List the risks and threats in wireless network.

9. Write a note on data confidentiality in IOT environment.

10. Differentiate between PaaS availability management- IaaS availability management.

PART B — (5 × 13 = 65 marks)

11. (a) (i) Illustrate in detail about Euclidean Algorithm with examples. (7)

(ii) Describe in detail about Chinese remainder theorem with its two assertions. (6)

Or

(b) Explain in detail about the security design principles, attack surfaces and trees with an example application.

12. (a) Consider a Diffie-Hellman scheme with a common prime q = 11 and a primitive root $\alpha = 2$.

(i) If user A has public key $Y_A = 9$, what is A's private key X_A? (6)

(ii) If user B has public key $Y_B = 3$, what is the shared secret key K? (7)

Or

(b) (i) Illustrate in detail about RSA algorithm with an example. (7)

(ii) Show that Feistel decryption is the inverse of Feistel encryption. (6)

13. (a) (i) Explain in detail about the working nature of Secure Hash Algorithm (SHA). (6)

(ii) Describe about HMAC algorithm and structure with example. (7)

Or

(b) (i) Exemplify in detail about PKIX Architectural Model. (6)

(ii) Describe about the access control principles policies and access rights. (7)

14. (a) Illustrate in detail about the virtualization security with its native and hosted virtualization security layers diagram and its issues.

Or

(b) (i) Elaborate in detail about the Wireless LAN Security with diagram. (7)

(ii) Exemplify about the wireless security architectures and security tools. (6)

15. (a) Discuss in depth about the IOT security architecture, challenges. requirements and its future.

Or

(b) Explain in detail about Cloud Security Architecture, its different variants and access controls.

PART C — (1 × 15 = 15 marks)

16. (a) Consider a company whose operations are housed in two buildings on the same property, one building is headquarters the other building contains network and computer services. The property is physically protected by a fence around the perimeter. The only entrance to the property is through the fenced perimeter In addition to the perimeter fence, physical security consists of a guarded front gate. The local networks are split between the Headquarters' LAN and the Network Services' LAN. Internet users connect to the Web server through a firewall. Dial-up users get access to a particular server on the Network Services LAN. Develop an attack tree in which the root node represents disclosure of proprietary secrets. Include physical social engineering, and technical attacks. The tree may contain both AND and OR nodes. Develop a tree that has at least 15 leaf nodes.

Or

(b) Suppose that someone suggests the following way to confirm that the two of you are both in possession of the same secret key. You create a random bit string the length of the key, XOR it with the key, and send the result over the channel. Your partner XORs the incoming block with the key (which should be the same as your key) and sends it back. You check, and if what you receive is your original random string, you have verified that your partner has the same secret key, yet neither of you has ever transmitted the key. Is there a flaw in this scheme? Defend your answer.

———————