SRM VALLIAMMAI ENGINEERING COLLEGE

(An Autonomous Institution)

SRM Nagar, Kattankulathur – 603 203

DEPARTMENT OF ARTIFICIAL INTELLIGENCE & DATA SCIENCE

QUESTION BANK

IV SEMESTER

AD3462 – DATA AND INFORMATION SECURITY

Regulation – 2023

Academic Year 2025 – 2026 (EVEN)

Prepared by

Mr. S. Srinivasan, Professor of Practice, AI&DS

Ms. M. Abinaya, Assistant Professor, AI&DS

SRM VALLIAMMAI ENGINEERING COLLEGE

(An Autonomous Institution)

SRM Nagar, Kattankulathur – 603 203.

DEPARTMENT OF ARTIFICIAL INTELLIGENCE & DATA SCIENCE

QUESTION BANK

SUBJECT : AD3462 & DATA AND INFORMATION SECURITY
YEAR/SEM : II Year / IV Semester

UNIT I INTRODUCTION

History, what is Information Security? Critical Characteristics of Information, NSTISSC Security Model, Components of an Information System, Securing the Components, Balancing Security and Access, The SDLC, The Security SDLC

PART – A

Q.No	Questions	BT Level	Competence
1	How shall you interpret Information Security?	BTL2	Understand
2	What is the difference between vulnerability and exposure?	BTL2	Understand
3	What is the difference between a threat agent and a threat?	BTL2	Understand
4	What are the three components of the C.I.A. triad? What are they used for?	BTL2	Understand
5	Give the critical characteristics of Information	BTL1	Remember
6	List the characteristics of CIA triangle	BTL1	Remember
7	What are the main components of an information system?	BTL2	Understand
8	Differentiate direct and indirect attack	BTL2	Understand
9	What are the measures required to protect confidentiality of information?	BTL1	Remember
10	Name the multiple layers of security that a successful organization should have in its place to protect its operations	BTL2	Understand
11	How shall you design the computer as the subject and object of the attack?	BTL2	Understand
12	How Did Cyber Security Start?	BTL1	Remember
13	Examine if the C.I. triangle is incomplete, why is it so commonly used in security?	BTL2	Understand
14	Trace the history of information security	BTL1	Remember
15	What is Security? What are the security layers, a successful organization should implement?	BTL2	Understand
16	Write about NSTISSC Security model.	BTL1	Remember
17	write about People components of an information system	BTL2	Understand
18	What is meant by balancing Security and Access?	BTL2	Understand
19	Define the Security SDLC and its importance in information security.	BTL1	Remember
20	State the responsibilities of Data Owners, Data custodians and Data users.	BTL2	Understand
21	What is Malware? How did it start?	BTL2	Understand
22	How can the practice of information security be described as both an art and a science?	BTL2	Understand
23	Who should lead a security team? Should the approach to security be more managerial or technical?	BTL2	Understand
24	Why is the top-down approach to information security superior to the bottom-up approach?	BTL2	Understand
PART-B			
1	Identify the six components of an information system. Which are most directly	BTL5	Evaluate

	affected by the study of computer security? Which are most commonly associated with its study?		
2	Describe the critical characteristics of information. How are they used in the study of computer security?	BTL3	Apply
3	Why is a methodology important in the implementation of information security? How does a methodology improve the process?	BTL3	Apply
4	How has computer security evolved into modern information security?	BTL4	Analyze
5	Show and explain with the help of a diagram about the components of information Security	BTL3	Apply
6	Analyze the critical characteristics of information. How are they used in the study of computer security?	BTL3	Apply
7	i). What is NSTISSC Security Model? (8) ii). Describe in detail about the top down approach and the bottom up approach with the help of a diagram.(8)	BTL4	Analyze
8	i)List the various components of an information system and tell about them. (8) ii)List the history of Information Security.(8)	BTL4	Analyze
9	Evaluate the various components of Information Security that a successful organization must have.	BTL4	Analyze
10	i). Infer about Information Security Project Team. (8) ii) Analyze the methodology important in the implementation of information security? How does a methodology improve the process? (8)	BTL4	Analyze
11	Formulate any methodology, why it important in the implementation of information security? How does a methodology improve the process?	BTL4	Analyze
12	i)Compose the roles of Information Security Project Team. ii)Design the steps unique to the security systems development life cycle in all the phases of SSDLC model.	BTL4	Analyze
13	What is SDLC? Explain different phases of SDLC	BTL4	Analyze
14	What is Security SDLC? Explain its different phases.	BTL5	Evaluate
15	Describe the information security roles to be played by various professionals in a typical organization?	BTL5	Evaluate
16	Illustrate briefly about SDLC waterfall methodology and its relation in respect to information security.	BTL6	Create
17	Explain CIA triad in detail. How does each component contribute to data and information security	BTL4	Analyze

UNIT II SECURITY INVESTIGATION

Need for Security, Business Needs, Threats, Attacks, Legal, Ethical and Professional Issues - An Overview of Computer Security - Access Control Matrix, Policy-Security policies, Confidentiality policies, Integrity policies and Hybrid policies

PART – A

Q.No	Questions	BT Level	Competence
1	Examine the meaning of the sentence “data in motion and data at rest”.	BTL2	Understand
2	List the four important functions ,the information security performs in an organization?	BTL1	Remember
3	Analyze the assets in the organization that requires protection	BTL2	Understand
4	Why is data the most important asset an organization possesses? What other assets in the organization require protection?	BTL2	Understand
5	What is meant by the term “Information Extortion”?	BTL1	Remember

6	What are the three general categories of unethical and illegal behavior?	BTL1	Remember
7	Illustrate the technical mechanisms that have been used to enforce copyright laws	BTL1	Remember
8	Analyze the major differences between a Threat and an Attack.	BTL2	Understand
9	What is malware. Breifly explain it.	BTL2	Understand
10	Construct with the help of a table any 4 threats with its examples.	BTL1	Remember
11	Name the most common methods of virus transmission.	BTL1	Remember
12	Define the following terms: Macro Virus & Boot Virus	BTL1	Remember
13	Analyze about commonplace security principles.	BTL2	Understand
14	State the various types of malware? How do worms differ from viruses?	BTL2	Understand
15	What is Trojan horses attack. Do they carry viruses or worms?	BTL2	Understand
16	Define the meaning of the term 'Electronic Theft'	BTL2	Understand
17	List any five attacks that is used against controlled systems.	BTL2	Understand
18	Express about the password attacks	BTL2	Understand
19	What is DoS attack? How can the organizations prevent it?	BTL2	Understand
20	What is Access Control Matrix.	BTL2	Understand
21	What is a security policy document? Briefly explain what it addresses.	BTL2	Understand
22	How can you protect against shoulder surfing?	BTL2	Understand
23	Define Private and Public Law.	BTL2	Understand
24	How do confidentiality policies differ from integrity policies in information security?	BTL2	Understand
	PART-B		
1	For a sniffer attack to succeed, what must the attacker do? How can an attacker gain access to a network to use the sniffer system?	BTL6	Create
2	Illustrate the methods does a social engineering hacker use to gain information about a user's login id and password? How would this method differ if it were targeted towards an administrator's assistant versus a data-entry clerk?	BTL6	Create
3	How has the perception of the hacker changed over recent years? Compose the profile of a hacker today by depicting the violated techniques, algorithms and security protocols.	BTL6	Create
4	a. List the Computer Security Hybrid Polices and explain (8) b. Describe the types of Computer Security (8)	BTL3	Apply
5	Illustrate which management groups are responsible for implementing information security to protect the organization's ability to function. Depict Access control architecture for e-commerce company by assuming role and responsibilities	BTL6	Create
6	What is Cybersecurity? What are the elements of cyber security? What are the common Cyberattacks?	BTL3	Apply
7	What are the various types of malware? How do worms differ from viruses? Do Trojan horses carry viruses or worms?	BTL4	Analyze
8	What is the difference between a denial-of-service attack and a distributed denial of- service attack? Which is more dangerous? Why? Explain by depicting them and how it can be prevented?	BTL4	Analyze
9	What are the various forces of nature? Which type might be of greatest concern to an organization in Chennai? Bangalore? Delhi? Mumbai?	BTL5	Evaluate
10	What is intellectual property? Does the intellectual property owned by an organization usually have value? If so, how can attackers threaten that value?	BTL4	Analyze
11	What are the emerging trends in security investigations? Discuss how advancements in AI, machine learning, and blockchain are influencing the field.	BTL4	Analyze
12	i) State the types of password attacks. (8) ii) ii)Tell the three ways in which an authorization can be handled.(8)	BTL4	Analyze
13	Point out why data the most important asset an organization possesses? What other assets in the organization require protection and how?	BTL5	Evaluate

14	i)	BTL5	Evaluate
15	i)Explain Integrity Policies. (8) ii) What is a buffer overflow, and how is it used against a Web server?(8)	BTL5	Evaluate
16	Generalize how the intellectual property owned by an organization usually have value? If so, how can attackers threaten that value?	BTL4	Analyze
17	How will you develop management groups that are responsible for implementing information security to protect the organization's ability to function ?	BTL6	Create

UNIT III DIGIAL SIGNATURE AND AUTHENTICATION

Digital Signature and Authentication Schemes: Digital Signature-Digital Signature Schemes and their Variants- Digital Signature Standards-Authentication: Overview- Requirements Protocols - Applications - Kerberos -X.509 Directory Services 83.

PART – A

Q.No	Questions	BT Level	Competence
1	List the properties of digital signature	BTL1	Remember
2	Explain the types of attacks.	BTL1	Remember
3	List the forgeries done by attacker to break the break the digital signature	BTL2	Understand
4	What is meant by primitive root?	BTL1	Remember
5	Given two integers A=3 and M=11, identify the modular multiplicative inverse of A under modulo M.	BTL1	Remember
6	Identify the primitive roots of a prime number q=7.	BTL1	Remember
7	Compare RSA approach and DSA approach.	BTL2	Understand
8	Define Kerberos and its Requirements	BTL2	Understand
9	List the characteristics of user certificate generated by CA.	BTL1	Remember
10	Explain different authentication mechanisms.	BTL2	Understand
11	What are the requirements of a good authentication protocol?.	BTL1	Remember
12	Explain the Key distribution center.	BTL1	Remember
13	What is the role of hashing algorithms in digital signatures?	BTL2	Understand
14	Discuss the three threats that may occur in a workstation	BTL2	Understand
15	List the requirements that are not satisfied by version 2 of X.509 certificate.	BTL2	Understand
16	List the categories of certificate extensions.	BTL2	Understand
17	List the difference between Symmetric and Asymmetric Key encryption	BTL2	Understand
18	What are the major challenges of Symmetric cryptography?	BTL2	Understand
19	List four requirements for the distribution using public key cryptography?	BTL2	Understand
20	What types of certificates does anX.509 CA's directory entry contain?	BTL2	Understand
21	What are the three general Authentication Factors	BTL2	Understand
22	List advantages and drawbacks of remote user authentication.	BTL2	Understand
23	What entities constitute a full service Kerberos environment?	BTL2	Understand
24	List the different approaches to attack the RSA algorithm	BTL2	Understand
	PART-B		
1	Explain Elgamal Digital Encryption Scheme.	BTL3	Apply
2	Explain NIST Digital Signature Algorithm	BTL3	Apply
3	a. What are the methods of public key distribution? (8) b. Which of the public key distribution systems is most secure? (4) c. How many handshake rounds are required in the public-key distribution scenario?(4)	BTL6	Create
4	Explain Elliptic curve Digital Signature Algorithm.	BTL3	Apply

5	Explain Schnorr Digital Encryption Scheme	BTL3	Apply
6	Outline RSA-PSS Digital signature algorithm.	BTL3	Apply
7	Outline the working of X.509 certificate along with its format.	BTL4	Analyze
8	Explain briefly about Kerberos.	BTL4	Analyze
9	Explain the categories of certificate extensions in X.509 certificates	BTL4	Analyze
10	a. Can you explan what a key distribution center(KDC) is in the context of Kerberos? (8) b. Why do we need to use double encryption when using Kerberos (4) c. What are some advanantages and disadvanateges of using Kerberos for authentication.(4)	BTL5	Evaluate
11	a. Can you explain what mutual authentication means in the context of Kerberos (8) b. What is pass the hash attack? How does it affect Kerberos? (4) c. What are common federated identity management (FIM) use cases.(4)	BTL5	Evaluate
12	Discuss the role of a Certificate Authority (CA) in a Public Key Infrastructure (PKI). How does the CA ensure trust in digital signatures?	BTL4	Analyze
13	a. What is the maximum number of handshake? (4) b. How is X509 validated? (6) c. How do we identify a X509 certificate? (6)	BTL5	Evaluate
14	a. What types of attacks can be used against Kerberos? (6) b. What happens if an entry is deleted from the active directory database? (5) c. Are there any limitations on the number of keys that a user can request and what is the limitation if yes? (5)	BTL5	Evaluate
15	Explain the Digital Signature Standards(DSS) with diagrams and its components.	BTL5	Evaluate
16	Evaluate the security challenges associated with digital signatures. How can attacks such as key compromise, hash collision, and certificate forgery be mitigated?	BTL5	Evaluate
17	a. What is the difference between a digital signature and an electronic signature? (6) b. What is the difference between direct and arbitrated digital signatures? (5) c. What are some threats associated with a direct digital signatures? (5)	BTL6	Create

UNIT IV E-MAIL AND IP SECURITY

E-mail and IP Security: Electronic mail security: Email Architecture -PGP – Operational Descriptions- Key management- Trust Model- S/MIME.IP Security: Overview- Architecture - ESP, AH Protocols IPSec Modes – Security association - Key management.

PART – A

Q.No	Questions	BT Level	Competence
1	Discuss about the purpose of padding field in ESP.	BTL1	Remember
2	Explain the usage of Mail Submission Agent.	BTL1	Remember
3	Explain “must” and “should” terminology in S/MIME.	BTL2	Understand
4	List the IPsec services.	BTL1	Remember
5	Explain the usage of usage of Message Transfer Agent.	BTL1	Remember
6	Describe replay attack.	BTL1	Remember
7	Explain the advantages of using Authentication header?	BTL2	Understand
8	Explain the applications of IPV6.	BTL2	Understand
9	Mention the benefits and limitations of S/MIME in email security.	BTL1	Remember
10	Explain the two additional fields in payload of ESP.	BTL1	Remember

11	What is the key concept of Security Association(SA) in IP Security Policy?	BTL2	Understand
12	What is PGP?	BTL1	Remember
13	What is the role of key management in PGP?.	BTL2	Understand
14	Mention four SSL protocols	BTL2	Understand
15	Explain the reasons for using PGP?	BTL2	Understand
16	What are the protocols used to provide IP security?	BTL2	Understand
17	Specify the IP security services?	BTL2	Understand
18	What is the difference between TLS and SSL security?	BTL2	Understand
19	Give the benefits of IP security?	BTL2	Understand
20	What do you mean by Security Association? Specify the parameters that identifies the Security Association?	BTL2	Understand
21	What are all the steps involved in SSL required protocol?	BTL2	Understand
22	Define: Truncation Attack	BTL2	Understand
23	Purpose of id payload in ISAKMP/IKE encoding?	BTL2	Understand
24	List the limitations of SMTP/RFC 822?	BTL2	Understand
	PART-B		
1	Explain S/MIME operational descriptions, message content types and enhanced security services.	BTL3	Apply
2	Explain AH protocol with its format and modes.	BTL3	Apply
3	Illustrate email architecture and explain its protocols.	BTL4	Analyze
4	Explain the various IPsec components with a neat architecture diagram. Also explain the IPsec modes.	BTL3	Apply
5	Explain all the fields in Authentication Header with its two modes.	BTL4	Analyze
6	Illustrate the ESP along with its modes	BTL3	Apply
7	Explain the steps, methodology involved in SSL/TLS protocol?	BTL3	Apply
8	Using the comparison table, describe an example of how SMTP, POP3, and IMAP correlate with and differ from each other.	BTL6	Create
9	a. What does domain name system security extensions(SNSSEC) protect against? (8) b. Does email use data? Explain.(8)	BTL5	Evaluate
10	What are the key principles of firewall security in protecting IP networks? Compare different types of firewalls (e.g., packet-filtering, stateful inspection, application-layer) and their effectiveness in different scenarios.	BTL4	Analyze
11	What is Encapsulating Security Payload ?	BTL4	Analyze
12	Write down the Difference between PGP and S/MIME	BTL4	Analyze
13	Write the details on Authentication Header (AH) format.	BTL5	Evaluate
14	What is the process to transfer a public key certificate using IKE? What happens when SA is deleted?	BTL5	Evaluate
15	Explain the mechanisms of email encryption (e.g., S/MIME, PGP) and email encryption how they ensure the confidentiality and integrity of email communications. What are the challenges associated with their adoption?	BTL5	Evaluate
16	Explain in detail about architecture of IP Security. Depict how email message could be sent secured with neat example.	BTL6	Create
17	Explain the operation description of PGP. Provide real time case study for understanding its real time working	BTL6	Create

UNIT V WEB SECURITY

Web Security: Requirements- Secure Sockets Layer- Objectives-Layers -SSL secure Communication-Protocols - Transport Level Security. Secure Electronic Transaction- Entities DS Verification-SET processing.

PART – A

Q.No	Questions	BT Level	Competence
1	Compare Passive and Active web security attacks.	BTL2	Understand
2	List the parameters of connection state in TLS.	BTL2	Understand
3	List the parameters of session state in TLS.	BTL2	Understand
4	Explain SET protocol.	BTL2	Understand
5	Discuss how the TLSV1.3 differs from its previous version?	BTL2	Understand
6	Compare TLS connection and TLS Session.	BTL2	Understand
7	Explain change cipher spec protocol.	BTL1	Remember
8	Explain the ways of classifying web security threats	BTL1	Remember
9	Explain S-HTTP.	BTL1	Remember
10	How is SSL used to protect web applications from security vulnerabilities?	BTL1	Remember
11	What is chosen-plaintext attack?	BTL1	Remember
12	Explain 2012 CRIME.	BTL1	Remember
13	What is PGP?	BTL2	Understand
14	Explain the purpose of alert protocol.	BTL2	Understand
15	Outline the final step of TLS Record protocol	BTL2	Understand
16	List the top web security threats	BTL2	Understand
17	List and briefly define the SSH protocols	BTL2	Understand
18	Which protocol was replaced by SSH and why? Which version is currently in the process of being standardized.	BTL2	Understand
19	List benefits of TLS.	BTL2	Understand
20	What services are provided by TLS Record Protocol	BTL2	Understand
21	What steps are involved in the TLS Record Protocol transmission?	BTL2	Understand
22	List some major differences between SSL and TLS.	BTL2	Understand
23	What are the difference between SSL and SET.	BTL2	Understand
24	Explain the purpose of alert protocol.	BTL2	Understand

PART-B

1	Explain the following protocols i) TLS record protocol (8) ii) Heartbeat protocol (8)	BTL3	Apply
2	i) Explain the secure socket layer and working of SSL protocol (8) ii) Explain the categories of web security threats that affects the integrity, authenticity, confidentiality and availability and explain its consequences and countermeasures. (8)	BTL3	Apply
3	Outline Transport level security architecture and explain its protocols	BTL4	Analyze
4	Explain the protocols for securing internet communication, email and web transactions.	BTL4	Analyze
5	Explain the working of Handshake protocol.	BTL3	Apply
6	You are developing a web application where users can chat securely with one another. The application will send messages over the internet, and you want to ensure that these messages remain private and unaltered during transit. Describe how you would apply Transport Level Security (TLS) in your application to protect	BTL6	Create

	the messages. Discuss how the two layers of protocols in TLS architecture would participate in establishing and maintaining this secure communication		
7	a. What is difference between SSH and Telnet? (6) b. What is the difference between HTTP and HTTPS? (6) c. Which SSL protocol consist of only 1 bit. (4)	BTL4	Analyze
8	a. What are the authentication levels of secure socket layer(SSL) / transport layer security(TLS) certificates? (10) b. What is the difference between HTTP and HTTPS(6)	BTL4	Analyze
9	Explain in details the Transport Layer Security(TSL).	BTL4	Analyze
10	Explain in detail the Secured Electronic Transaction(SET)	BTL4	Analyze
11	With the help of neat diagram explain the SET processing including the participants and the sequence of actions.	BTL4	Analyze
12	a. What are the authentication levels of secured socket layer(SSL) / transport layer security(TSL) certificates? (10) b. What purpose does the MAC serve during the change cipher spec TLS exchange? (6)	BTL4	Analyze
13	Details the major differences between SSL and TLS.	BTL5	Evaluate
14	What are the considerations of Web Security and detail the threats to the web security?	BTL6	Create
15	Explain the role of penetration testing in web security. How can organizations use penetration testing to identify and remediate vulnerabilities in their web applications?	BTL5	Evaluate
16	a) List some of the Common Web Security Threats (8) b) How to Implement Web Security Measures? (8)	BTL6	Create
17.	Explain the concept of SQL Injection and its impact on web applications. How can developers protect their applications from SQL Injection attacks?	BTL4	Analyze

****