Tutorial Sheet – Unit V

E-Mail Security, IP Security (IPSec), and Case Studies on Cryptography & Security

Part A: Short Answer Questions

E-Mail Security

1. What is E-Mail Security?
2. What are the major threats to e-mail communication?
3. What is PGP?
4. Expand PGP.
5. What are the services provided by PGP?
6. What is S/MIME?
7. Expand S/MIME.
8. What is a digital signature in e-mail security?
9. What is e-mail encryption?
10. What is message authentication in e-mail systems?
11. Differentiate between PGP and S/MIME.
12. What is MIME?

IP Security (IPSec)

13. What is IP Security (IPSec)?
14. Why is IPSec required?
15. Define Security Association (SA).
16. What is Authentication Header (AH)?
17. What is Encapsulating Security Payload (ESP)?
18. What security services are provided by AH?
19. What security services are provided by ESP?
20. What is transport mode in IPSec?
21. What is tunnel mode in IPSec?
22. What is Internet Key Exchange (IKE)?
23. What is the purpose of IKE?
24. What is IPSec architecture?
25. What is anti-replay protection?

Case Studies

26. What is Secure Multiparty Computation?
27. What is a Virtual Election System?
28. What is Single Sign-On (SSO)?
29. What are the advantages of SSO?
30. What is a Cross-Site Scripting (XSS) attack?

31. What is a reflected XSS attack?
32. What is a stored XSS attack?
33. What is an inter-branch payment transaction system?
34. What is trust management in online transactions?
35. What is secure electronic voting?

Part B: Long Answer Questions

E-Mail Security

1. Explain the need for e-mail security.
2. Discuss various threats to e-mail communication.
3. Explain the architecture and services of PGP.
4. Describe the operation of PGP in secure e-mail communication.
5. Explain message encryption and authentication in PGP.
6. Discuss the advantages and limitations of PGP.
7. Explain the architecture and operation of S/MIME.
8. Describe how S/MIME provides confidentiality and authentication.
9. Compare PGP and S/MIME.
10. Explain digital signatures in e-mail security.

IP Security (IPSec)

11. Explain the overview and objectives of IPSec.
12. Describe the IPSec architecture with a neat diagram.
13. Explain Authentication Header (AH) and its operation.
14. Describe Encapsulating Security Payload (ESP) and its operation.
15. Compare AH and ESP.
16. Explain IPSec transport mode and tunnel mode.
17. Discuss Security Associations in IPSec.
18. Explain the concept of combining Security Associations.
19. Describe the Internet Key Exchange (IKE) protocol.
20. Explain IPSec key management and authentication mechanisms.
21. Discuss the advantages and limitations of IPSec.
22. Explain how IPSec provides confidentiality, integrity, and authentication.

Case Studies on Cryptography and Security

23. Explain Secure Multiparty Computation and its applications.
24. Discuss the concept and security requirements of Virtual Elections.
25. Explain the architecture and working of Single Sign-On (SSO).
26. Discuss the benefits and security challenges of SSO.
27. Explain secure inter-branch payment transaction systems.
28. Discuss cryptographic techniques used in banking transactions.

29. Explain Cross-Site Scripting (XSS) vulnerabilities.
30. Discuss different types of XSS attacks and their prevention.
31. Analyze the role of cryptography in secure online voting systems.
32. Explain the importance of authentication and authorization in SSO systems.

Part C: Analytical and Conceptual Questions

1. Why is e-mail security necessary in modern communication?
2. Analyze the advantages of PGP over traditional e-mail systems.
3. Compare PGP and S/MIME based on security services.
4. Why is ESP generally preferred over AH in IPSec implementations?
5. Analyze the importance of Security Associations in IPSec.
6. Compare IPSec transport mode and tunnel mode.
7. Why is IKE important in IPSec communication?
8. Analyze the role of cryptography in secure electronic voting.
9. Discuss the security benefits and limitations of Single Sign-On.
10. Why are Cross-Site Scripting attacks dangerous for web applications?
11. Analyze the cryptographic requirements of inter-branch banking transactions.
12. Discuss privacy challenges in Secure Multiparty Computation.

Part D: Problem-Solving and Application Questions

E-Mail Security

1. Draw and explain the architecture of PGP.
2. Illustrate the process of sending a secure PGP e-mail.
3. Draw the architecture of S/MIME and explain its operation.
4. Explain how digital signatures are used in secure e-mail communication.

IPSec

5. Draw the IPSec architecture and explain its components.
6. Explain the packet structure of Authentication Header (AH).
7. Explain the packet structure of Encapsulating Security Payload (ESP).
8. Illustrate IPSec transport mode with a neat diagram.
9. Illustrate IPSec tunnel mode with a neat diagram.
10. Explain the phases of Internet Key Exchange (IKE).

Case Studies

11. Design a secure electronic voting system using cryptographic techniques.
12. Illustrate the workflow of a Single Sign-On system.

13. Explain how secure multiparty computation protects private information.
14. Analyze a secure inter-branch payment transaction process.
15. Demonstrate a Cross-Site Scripting attack scenario and suggest preventive measures.

Part E: Multiple Choice Questions (MCQs)

1. PGP stands for:
    - A) Private Good Privacy
    - B) Pretty Good Privacy
    - C) Protected Global Privacy
    - D) Personal Global Protection

    Answer: B

2. S/MIME is primarily used for:
    - A) Routing
    - B) Secure E-Mail
    - C) VPN
    - D) DNS

    Answer: B

3. IPSec operates at:
    - A) Application Layer
    - B) Transport Layer
    - C) Network Layer
    - D) Data Link Layer

    Answer: C

4. AH provides:
    - A) Confidentiality
    - B) Authentication and Integrity
    - C) Compression
    - D) Routing

    Answer: B

5. ESP provides:
    - A) Confidentiality
    - B) Integrity
    - C) Authentication
    - D) All of the above

Answer: D

6. IKE stands for:
    - A) Internet Key Exchange
    - B) Integrated Key Encryption
    - C) Internet Kernel Exchange
    - D) Internal Key Engine

    Answer: A

7. Tunnel mode is commonly used in:
    - A) VPNs
    - B) FTP
    - C) DNS
    - D) SMTP

    Answer: A

8. SSO stands for:
    - A) Single Sign-On
    - B) Secure Sign-On
    - C) System Sign-On
    - D) Single Security Operation

    Answer: A

9. XSS stands for:
    - A) Cross Server Security
    - B) Cross Site Scripting
    - C) Cross System Service
    - D) Cross Security Standard

    Answer: B

10. Secure Multiparty Computation aims to:
    - A) Compress Data
    - B) Compute Functions While Preserving Privacy
    - C) Route Packets
    - D) Encrypt Images

    Answer: B

Part F: Assignment Questions

1. Study the architecture and operation of PGP.
2. Compare PGP and S/MIME in terms of functionality and security.
3. Analyze the IPSec protocol suite and prepare a report.
4. Compare AH and ESP protocols.
5. Study Internet Key Exchange (IKE) and explain its phases.
6. Investigate the use of IPSec in VPN technologies.
7. Analyze the role of cryptography in electronic voting systems.
8. Study Secure Multiparty Computation and its real-world applications.
9. Prepare a report on Single Sign-On technologies used in enterprises.
10. Investigate recent Cross-Site Scripting (XSS) vulnerabilities and prevention techniques.
11. Study secure banking transaction systems and cryptographic mechanisms used.
12. Compare different authentication mechanisms used in modern web applications.

Viva Questions

1. What is PGP?
2. What is S/MIME?
3. What are the services provided by PGP?
4. What is IPSec?
5. What is Authentication Header (AH)?
6. What is Encapsulating Security Payload (ESP)?
7. What is a Security Association?
8. What is IKE?
9. What is transport mode in IPSec?
10. What is tunnel mode in IPSec?
11. What is Secure Multiparty Computation?
12. What is a Virtual Election System?
13. What is Single Sign-On?
14. What are the benefits of SSO?
15. What is Cross-Site Scripting?
16. What are the types of XSS attacks?
17. What is secure electronic voting?
18. What is the role of cryptography in banking transactions?
19. How does IPSec ensure confidentiality?
20. Why is e-mail security important?

Important University Exam Questions (Frequently Asked)

10-Mark Questions

1. Explain the architecture and services of PGP.
2. Describe the operation of S/MIME.
3. Explain IPSec architecture with a neat diagram.
4. Discuss Authentication Header (AH) and Encapsulating Security Payload (ESP).
5. Explain Internet Key Exchange (IKE) and Security Associations.
6. Compare AH and ESP.
7. Explain Secure Multiparty Computation and its applications.
8. Discuss Virtual Elections and their security requirements.
9. Explain Single Sign-On architecture and operation.
10. Discuss Cross-Site Scripting vulnerabilities and prevention mechanisms.

5-Mark Questions

1. Compare PGP and S/MIME.
2. Explain transport mode and tunnel mode in IPSec.
3. Describe Security Associations.
4. Explain SSO and its advantages.
5. Discuss XSS attacks.
6. Explain secure inter-branch payment transactions.