Code No: F-13925/N/AICTE

FACULTY OF ENGINEERING

B.E. (CSE) VI–Semester (AICTE) (New) (Backlog) Examinations, February/March 2024

Subject: Cryptography & Network Security

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

Note: (i) First question is compulsory and answer any four questions from the remaining six questions. Each question carries 14 Marks.
(ii) Answer to each question must be written at one place only and in the same order as they occur in the question paper.
(iii) Missing data, if any, may be suitably assumed.

1. (a) Differentiate between Active attacks and Passive Attacks.
   (b) Write about Security Mechanisms in cryptography.
   (c) Mention the strengths and weakness of DES algorithm.
   (d) What do you mean by Asymmetric Key Cryptography?
   (e) What is the need of Data Integrity explain in brief.
   (f) Explain SSL Architecture in brief.
   (g) Explain in brief about IPSec, System Security.

2. Discuss the following:
   (a) Message Integrity (b) Denial of Service (c) Availability (d) Authentication (e) Diffusion & Confusion (f) steganography, confidentiality and authentication.

3. (a) Explain Euclidean and extended Euclidean Algorithms.
   (b) Write a note on Block Cipher Design Principles.

4. (a) Explain RSA cryptosystem and its different attacks.
   (b) Explain in detail (i) message authentication code and (ii) the requirements of MAC

5. (a) Discuss the working of Diffie-Hellman key exchange technique.
   (b) Differentiate the trade-off between symmetric key distribution and Kerberos.

6. (a) What is PGP? Show the Packet and Message format of PGP? Illustrate the key rings and its significance in PGP.
   (b) Infer the overall function of TLS

7. Write short note on (any TWO)
   (a) Security Goals
   (b) Digital Signature
   (c) Firewalls

******

Code No: E-5901/N/AICTE

FACULTY OF ENGINEERING

B.E. (CSE) VI– Semester (AICTE) (Main) (New) Examinations, September/October 2023

Subject: Cryptography and Network Security

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

Note: (i) First question is compulsory and answer any four questions from the remaining six questions. Each questions carries 14 Marks.
(ii) Answer to each question must be written at one place only and in the same order as they occur in the question paper.
(iii) Missing data, if any, may be suitably assumed.

1. (a) What do you mean by cryptographic Attacks?
   (b) Define modern Symmetric key ciphers.
   (c) Explain Asymmetric key cryptography.
   (d) Define Fermat's little theorem and explain its application.
   (e) List some features of the Whirlpool cryptographic hash function. What kind of compression function is used in Whirlpool?
   (f) Distinguish between two modes of IPSec.
   (g) Define S/MIME.

2. (a) Explain Network Goals and Network Services.
   (b) Which technique (cryptography or steganography) is used in each of the following cases for confidentiality?
      (i) student writes the answers to a test on a small piece of paper, rolls up the paper and inserts it in a ball-point pen, and passes the pen to another student.
      (ii) To send a message, a spy replaces each character in the message with a symbol that was agreed upon in advance as the character's replacement.

3. (a) Explain Data Encryption Standard with Block Diagram.
   (b) Explain the difference between symmetric and asymmetric cryptography system.

4. (a) Write an algorithm in pseudocode for the Chinese remainder theorem.
   (b) Define Data integrity and why it is required?

5. (a) Define the elliptic curve digital signature scheme and compare it to the elliptic curve cryptosystem.
   (b) Compare and contrast attacks on digital signatures with attacks on cryptosystems.

6. (a) Explain in detail about PGP PROTOCOL in detail.
   (b) When a session is resumed with a new connection, SSL does not require the full handshaking process. Show the messages that need to be exchanged in a partial handshaking.

7. (a) Define the RSA digital signature scheme and compare it to the RSA cryptosystem.
   (b) Define ISAKMP and List ISAKMP payload types and the purpose of each type.

****

Code No: E-5973/N/AICTE

FACULTY OF ENGINEERING

B.E. (IT) VI – Semester (AICTE) (Main) (New) Examinations, September/October 2023

Subject: Network Security & cryptography

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

Note: (i) First question is compulsory and answer any four questions from the remaining six questions. Each questions carries 14 Marks.
(ii) Answer to each question must be written at one place only and in the same order as they occur in the question paper.
(iii) Missing data, if any, may be suitably assumed.

1. (a) Define Active attacks and Passive attacks.
   (b) What are the differences between symmetric key and public key cryptography?
   (c) Define Blowfish algorithm.
   (d) Define CMAC function.
   (e) What is Handshake protocol in SSL?
   (f) What are Transport mode ESP and Tunnel mode ESP?
   (g) List the Applications of IPsec.

2. (a) What is network security? Explain model for network security with diagram.
   (b) What are the different substitution techniques? Explain any one in detail.

3. (a) Draw the Block diagram of DES and explain.
   (b) Explain RSA algorithm with example.

4. (a) Draw HMAC structure and explain.
   (b) What is digital signature? Explain Digital signature standard in detail.

5. (a) Explain in detail IEEE 802.11i LAN security.
   (b) Describe Wireless transport layer security Protocol Stack.

6. (a) Explain how Transmission and Reception of PGP Messages are done.
   (b) What is the requirement of IP security? Explain the architecture of IP security.

7. (a) Explain how symmetric key distribution is done using symmetric encryption.
   (b) Explain the functionality of S/MIME.

****

FACULTY OF ENGINEERING

Code No: E-5451/AICTE

B.E. (IT) VIII - Semester (AICTE) (Main & Backlog) Examination, June 2023

Subject: Cryptography & Network Security (P.E-VI)

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

(Missing data, if any, may be suitably assumed)

PART – A

Note: Answer all the questions. **(10 x 2 = 20 Marks)**

1. List the types of Security attacks.
2. Discuss the impact of key size on the robustness of an encryption algorithm.
3. Describe block cipher principles.
4. List any four symmetric key cipher methods.
5. Differentiate between block cipher and stream cipher.
6. List the advantages of TLS over SSL.
7. Differentiate between transfer mode and tunnel mode.
8. List the transfer encoding provided by SMIME.
9. Write about wireless LAN Security.
10. Discuss ESP (Encapsulating security payload).

PART – B

Note: Answer any five questions. **(5 x 10 = 50 Marks)**

11. (a) Explain any four substitution ciphers and discuss their advantages and disadvantages.
    (b) List and explain the six principles of Network Security.

12. (a) Write and explain the working of Diffie-Hellman key exchange algorithm.
    (b) Describe transposition cipher.

13. (a) Explain the working of RSA algorithm with example.
    (b) Write about secure Hash Algorithm (SHA-512) in detail.

14. Explain following security protocols
    (a) Kerberos
    (b) X.509 security protocols

15. Write in detail about
    (a) Secure socket layer security
    (b) Transport layer securities

16. (a) Discuss IEEE802.11 and IEEE802.11i in detail.
    (b) Explain about SSH wireless security.

17. (a) Write about SMIME IP Security in detail.
    (b) Explain Authentication Header.

******