Dronacharya College of Engineering, Gurgaon

Department of Electronics and Computers Engineering

Session 2014-2015

Subject: Information Security Systems (Code: EC-615-F)

Semester: VI/ Branch: ECS

Assignment-Section A

1. Define symmetric-key cipher. Distinguish between substitution and transposition cipher.
2. Brief about security mechanisms.
3. Define terms: Confidentiality and Availability.
4. What is product cipher?
5. For each of the following ciphers, say whether it is a stream cipher or block cipher. Defend your answers:
   - **a.** Playfair
   - **b.** One-time pad

Assignment-Section B

1. List names of mono-alphabetic and poly-alphabetic ciphers (two from each).
2. What do you mean by the term: "Denial of Service (DoS)".
3. List and briefly define categories of security mechanisms.
4. A message has 2000 characters. If it is supposed to be encrypted using a block cipher of 64 bits, find the size of the padding and the number of blocks.
5. Use the playfair cipher to encipher the message "The key is hidden under the door pad". The secret key can be made by filling the first and part of the second row the word "GUIDANCE" and filling the rest of the matrix with the rest of the alphabet

Assignment-Section C

6. Write short notes on transposition cipher.
7. Differentiate cryptography and steganography.
8. Encrypt and decrypt the message: "life is full of surprises" using the following ciphers:
   a. Caesar
   b. Playfair
   c. Monoalphabetic
9. Explain Columnar Transposition
10. Describe in brief the following terms: Non-repudiation, Authentication, and Integrity

11. How many padding bits must be added to a message of 100 characters, if 8-bit ASCII is used for encoding and the block cipher accepts blocks of 64-bits. Also find number of blocks.

Assignment-Section D

1. Explain OSI security architecture.
2. Differentiate between active and passive attacks.
3. Explain DES encryption technique in detail.
4. Explain symmetric and asymmetric cipher techniques.
5. Differentiate between block and stream ciphers in detail.
6. Discuss about Modular Arithmetic vs Euclid's Arithmetic.
7. Given polynomials f(x) = x3+x2+2 and g(x)= x2+x-1. Is g(x) a factor of f(x)? Show all of your calculations.

Important Questions

1. Define symmetric-key cipher. Distinguish between substitution and transposition cipher.
2. Brief about security mechanisms.
3. Define terms: Confidentiality and Availability.
4. What is product cipher?
5. For each of the following ciphers, say whether it is a stream cipher or block cipher. Defend your answers:
   - **c.** Playfair
   - **d.** One-time pad
   - **e.** Rotor
   - **f.** Enigma
6. List names of mono-alphabetic and poly-alphabetic ciphers (two from each).
7. What do you mean by the term: "Denial of Service (DoS)".
8. List and briefly define categories of security mechanisms.
9. A message has 2000 characters. If it is supposed to be encrypted using a block cipher of 64 bits, find the size of the padding and the number of blocks.
10. Use the playfair cipher to encipher the message "The key is hidden under the door pad". The secret key can be made by filling the first and part of the second row the word "GUIDANCE" and filling the rest of the matrix with the rest of the alphabet.
11. Write short notes on transposition cipher.
12. Differentiate cryptography and steganography.
13. Encrypt and decrypt the message: "life is full of surprises" using the following ciphers:
    a. Caesar
    b. Playfair
    c. Monoalphabetic

d. Columnar Transposition

14. Describe in brief the following terms: Non-repudiation, Authentication, and Integrity
How many padding bits must be added to a message of 100 characters, if 8-bit ASCII is used for encoding and the block cipher accepts blocks of 64-bits. Also find number of blocks.
15. Which security mechanism(s) are provided in each of the following cases?
   a. A company demands employee identification and a password to let employee log into the company server.
   b. A company server disconnects an employee, if he is logged into the system for more than two hours.
   c. A teacher refuses to send students grades by email unless they provide identification assigned by the teacher.
   d. A bank requires the customer's signature for a withdrawal.
16. List important design considerations for a stream cipher.
17. Define crypt analysis. Explain various types of crypt analytic attacks.
18. Explain OSI security architecture.
19. Differentiate between active and passive attacks.
20. Explain DES encryption technique in detail.

21. Explain symmetric and asymmetric cipher techniques.
22. Differentiate between block and stream ciphers in detail.
23. Discuss about Modular Arithmetic vs Euclid's Arithmetic.
24. Given polynomials f(x)=x3+x2+2 and g(x)=x2+x-1. Is g(x) a factor of f(x)? Show all your calculations.

25. Define finite field of order p. Show arithmetic in GF(7), that is, addition modulo 7, multiplication modulo 7, and additive and multiplicative inverses modulo 7.

26. Give the steps for constructing GF(2m) and hence give the elements of GF(24).

27. What is triple DES? What is triple DES with two keys? What is triple DES with three keys? Write AES algorithm for encryption. How does AES differ from DES?

28. State the prove Euler's theorem. How is RSA algorithm implemented? What are various approaches to attack RSA?

29. Using the Euclidean algorithm, find the greatest common divisor of the following:
i) 300 and 42
ii) 88 and 220

30. Find the results of the following, using Fermat's little theorem.
i) 515 mod 13
ii) 151 mod 17

31. What are the requirements of public key cryptography system? Explain the characteristic of

public key cryptography.

32. Explain Diffie-Hellman key exchange algorithm. In the Diffie- Hellman protocol, what happens if x and y have same value, that is Rita and Shyam have accidentally chosen the same number? Are R1 and R2 the same? Do the session keys calculated by Rita and Shyam have the same value? Give an example to prove your claims.

33. What is message digest? Write MD5 message digest algorithm. Compare the differences between MD-5 and SHA.

34. RC4 is the most widely-used software stream cipher and is used in popular protocols such as Secure Sockets Layer and WEP. Explain, how pseudorandom stream of bits are generated using RC4.

35. What is digital signature? Discuss a method to prepare digital signature.
36. What is a firewall and what are its limitations? What are the types of firewall? Discuss.
37. How is Authentication achieved in Pretty Good Privacy?
38. What is S/MIME and how does it works? Briefly explain.
39. How does IPSec offer the authentication and confidentiality service?
40. Discuss about the X.509 framework for the provision of Authentication Service.
41. Discuss basic requirements for Kerberos services.
42. Describe the authentication dialogue used by Kerberos for obtaining required services.
43. Explain the format of the X.509 certificate.
44. Discuss about the application and advantages of IPSec.