Part I - IS (FYMCA)

1. How are threat and vulnerability defined?
2. What is CIA (Confidentiality, Integrity and Availability)? (Refer L1-Information security ppt)
3. Compare Authentication and Authorization.
4. Compare between stream cipher and block cipher. Why is it important to study Feistel cipher? (Book- By William Stallings)
5. Write AES key expansion algorithm. (Book- By William Stallings)
6. Briefly describe AddRoundKey transformation in AES. (Book- By William Stallings)
7. Briefly describe the key expansion algorithm of AES. (Book- By William Stallings)
8. Compare between public key cryptosystems and private key cryptosystems. (Book- By William Stallings)
9. Which are different block cipher modes of operation? Give application of each.
10. Explain output feedback mode operation.
11. Define TRNG, PRNG and PRF.
12. Apply RSA algorithm to encrypt and decrypt following data.  
    p = 3, q = 11, e = 7, M = 5
13. Apply AddRoundKey transformation of AES cryptosystem. Given 128 bits of state and 128 bits of the round key.

|  |  |  |  |
| --- | --- | --- | --- |
| 47 | 40 | A3 | 4C |
| 37 | D4 | 70 | 9F |
| 94 | E4 | 3A | 42 |
| ED | A5 | A6 | BC |

|  |  |  |  |
| --- | --- | --- | --- |
| AC | 19 | 28 | 57 |
| 77 | FA | D1 | 5C |
| 66 | DC | 29 | 00 |
| F3 | 21 | 41 | 6A |

1. Determine disadvantages of traditional authentication methods and find requirements of biometric security scheme?
2. ) i) Construct a Playfair matrix with the key *occurrences.*  
    ii) Apply Transposition technique to encrypt the message “this is online exam” with a rail fence technique.

1. Explain different three threats associated with user authentication over a network or Internet?
2. Explain different types of analysis adopted by intrusion detection and protection systems (IDPS)? What are the types of IDPS?
3. Which are the five principal services provided by PGP? Explain in brief the authentication and confidentiality operations of PGP.
4. Give applications of IP security. What are benefits of IP security?
5. Explain in brief IP security policy.
6. Which are different usages of IDS in system security.
7. How packet sniffing works in network layer attack?
8. How network layer attacks attempt to compromise network devices and protocol stacks?
9. Illustrate the terms content attack, buffer overflows and password cracking attempts in application layer attacks of OSI model.
10. Which best practices are used for network defense? Illustrate in brief.
11. What is meant by security procedure? Give example of security procedure.
12. Compare Authentication and Authorization. Which are the factors to response to the authentication challenge? Which are different types of authorization systems?
13. Describe storage infrastructure in detail.
14. What is role of   
    a) cost of security  
    b) performance  
    c) Availability  
    d) security  
     in designing an appropriate network.
15. How are threat and vulnerability defined?
16. Which are different types of attacks?
17. How packet sniffing works in network layer attack?
18. How network layer attacks attempt to compromise network devices and protocol

stacks?

1. Illustrate the terms content attack, buffer overflows and password cracking attempts

in application layer attacks of OSI model.

1. Why CIA (Confidentiality, Integrity and Availability) triad is not perfect? Which

models are used to overcome limitations of CIA triad?

1. Show AES encryption process with diagram. Describe all steps in the process.
2. Which are different AES transformation functions?
3. Briefly describe ShiftRows transformation in AES algorithm.
4. Briefly describe MixColumns transformation in AES.
5. Describe RSA algorithm.
6. Which are strengths and weaknesses of firewall?
7. Which points should be considered when building a rule set on firewall?
8. Describe core firewall functions.
9. What is goal of VPN? How a VPN works?
10. Compare biometrics authentication method with other authentication methods. What is spoofing and anti-spoofing in biometric system?
11. Determine the requirements of biometric security scheme? What is need of liveness detection system? Explain different biometric identification techniques.
12. Compare steganography, cryptography and watermarking.
13. Which are different block cipher modes of operation? Explain output feedback mode operation. Give application of it.
14. Describe in brief AES encryption process with diagram. Which are different steps required in AES algorithm.
15. Explain biometric authentication in brief? Which are physiological and behavioral biometrics? Write down applications of biometrics.
16. What is biometrics? Which are the problems with possession- or knowledge- based authentication approaches?
17. ~~Design a face recognition system using PCA or any other feature extraction method.~~Describe DES algorithm in brief with diagram.
18. Create an artificial neural network for classification of face recognition system.
19. Design a fingerprint recognition system using minutiae points.
20. Write fuzzy vault algorithm for template security.
21. Compare MD5 and SHA Hash functions.
22. Compare AES and DES. Which one is bit oriented? Which one is byte oriented?
23. Explain with examples the CBC and ECB modes of block ciphers.
24. What are properties of hash function? Explain role of hash function in security
25. What is the need for message authentication? List various techniques used for message authentication. Explain anyone.
26. What are the requirements of the cryptographic hash functions? Compare MD5 and SHA-1 hash functions.
27. What are Denial of Service Attacks? Explain any three types of DoS attacks in detail.

Part II - IS (FYMCA)

63. define message authentication code? How it works?

64. Write SHA algorithm. What are applications of it?

65. Write MD5 algorithm.

66. What are cryptographic hash functions? How cryptographic hash functions work? What are applications of it?

67. Explain Caesar cipher algorithm. Apply Caesar cipher algorithm to encrypt and decrypt following sentence using key = 4.  
‘government college of engineering cs’

68. Explain substitution cipher and transposition cipher.

69. Apply Mono-alphabetic substitution cipher to encrypt and decrypt the data ‘government college of engineering cs’.

Random alphabet substitution for plain alphabet is given below. Use this cipher alphabet for encryption.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Plain Alphabet** | | | | | | | | | | | | | | | | | | | | | | | | | |
| a | b | c | d | e | f | g | h | i | j | k | l | m | n | o | p | q | r | s | t | u | v | w | x | y | z |
| **Cipher Alphabet** | | | | | | | | | | | | | | | | | | | | | | | | | |
| q | w | e | r | t | y | u | i | o | p | a | s | d | f | g | h | j | k | l | z | x | c | v | b | n | m |