ST JOSEPH ENGINEERING COLLEGE, MANGALURU

An Autonomous Institution

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

SUBJECT: CRYPTOGRAPHY AND CYBER SECURITY
COURSE CODE: **21CSE607**

QUESTION BANK

MODULE-1

1) Define the following terms:
i) Cryptography ii) Ciphertext
iii)Encryption iv) Decryption (10 marks)

2) Draw the simplified model of symmetric encryption and explain it. (6 marks)

3) Distinguish between:
i) Confusion and Diffusion ii) Block cipher and Stream ciphers (6 marks)

4) Explain Ceasar Cipher with an example. (4 marks)

5) Perform simple cipher substitution for below message “meet me after the toga party” and explain the mathematical equations with key=3. (10 marks)

6) Encryption the plaintext “ELECTRONICS” using a Playfair cipher with a key “INDIA”. (4 marks)

7) Encrypt the plaintext “CRYPTOGRAPHY” using HILL CIPHER technique with key matrix

K=

9	4
5	7

and decrypt the same. (10 marks)

8) Encrypt the message “Meet me at the usual place at ten rather than eight O’ clock”. Using the hill cipher with key

9	4
5	7

show your calculations and result. (10 marks)

9) With a neat diagram explain the Feistel structure of DES method. (10 marks)
10) With a neat schematic, explain the DES encryption algorithm. (10 marks)
11) Differentiate substitution and transposition techniques (4 marks)
12) Explain in detail Polyalphabetic Ciphers. (8 marks)
13) With suitable example explain rail fence ciphering. (6 marks)
14) Explain the playfair cipher and its rules for the following example.
Keyword: MONARCHY Plaintext: CRYPTOGRAPHY (10 marks)
15) Using Hill Cipher technique encrypt the plain text “paymoremoney” using the key

$$\mathbf{K=}\begin{matrix} 17 & 17 & 5 \\ 21 & 1 & 21 \\ 2 & 2 & 19 \end{matrix}$$

(10 marks)

MODULE-2

1) With a neat diagram, explain the six ingredients of a public key cryptography. (6 marks)

2) With neat diagram explain Authentication and secrecy in public key cryptosystem. (6 marks)

3) What are the applications of public key cryptosystem? (6 marks)
4) Explain RSA algorithm operation in detail. Perform an encryption of plain text and decryption of cipher text using RSA algorithm for P=3, Q=11,e=7, and M=5. (10 marks)

5) Explain the Elgamal cryptosystem. (4 marks)
6) What requirements must a public key cryptosystem fulfill to be a secure algorithm? (4 marks)

7) Explain Diffie-Helman key exchange algorithm. Apply Diffie -Helman key exchange algorithm for q=71 its primitive root alpha=7.A's private key is 5.B's private key is 12.
Find i) A's public key ii) B's public key iii) shared secret key. (10 marks)

8) Perform encryption using RSA algorithm following P=3, Q =11,e=3 and M =9. (10 marks)

9) Evaluate a Diffie-Hellman key exchange concept for prime number q=71 and primitive root alpha=7.
i) If user A has private key XA=5 what is A's public key YA?
ii) If user B has private key XB=12.What is B's public key YB?
iii) What is a shared key? (10 marks)

10) Compare how the Diffe-Hellman key exchange algorithm is useful in evaluating the man-in-middle attack concept. (10 marks)

11) Consider an Elgamal scheme with common prime q=71,and primitive root alpha=7.
i) If B has private key YB=3 ,and A choose the random integer K=2,what is the ciphertext of M=30?
ii) If A now choose a different value of K o that the encoding of M =30 is C(59,C2) What is integer C2? (10 marks)

12) Explain Public -Key Cryptosystems (10 marks)
13) Explain the description of RSA algorithm. (10 marks)
14) Describe Elgamal Cryptographic systems. (10 marks)

MODULE 3

1) Summarize the applications of cryptographic hash functions. (6 marks)

2) Explain why a hash function used for message authentication needs to be secured. (10 marks)

3) With neat diagrams explain the use of the Hash function for message authentication. (10 marks)
4) Explain the Secure Hash Algorithm (SHA). (10 marks)

5) Explain Basic Uses of Message Authentication code (MAC) (8 marks)

6) Explain about attacks on MACs . (6 Marks)

7)What are Message Authentication Requirements? (6 marks)

8)What is Digital Signature? What are the requirements of a digital signature?   (6 marks)

9)Explain El Gamal Digital Signature Techniques.   (10 marks)

10)What are the applications of cryptographic hash functions. (10 marks)

11)How can you achieve message authentication using MAC? (8 marks)

12) What are the security requirements of cryptographic hash functions? (6 marks)

13)How can we create digital signature ? (2 marks)

14)What is the message authentication code ?   (2 marks)

MODULE-4

1) Define Cybercrime. (2 marks)

2) Differentiate cybersquatting, cyberwarfare, cyberpunk and cyberterrorism. (8 marks)

3) Differentiate Information Security and Cyber Security. (5 marks)

4) Who is called as Cybercriminal? (2 marks)

5) Explain the three categories of cybercriminals. (5 marks)

6) How do you classify cybercrimes. Explain each in detail. (10 marks)

7) Discuss a) email spoofing b) data diddling c) salami attack d) web jacking e) online frauds. (10 marks)

8) Discuss about the global perspectives on Indian crimes.(8 marks)

9) Discuss the Indian ITA act 2000 and cybercrimes. (8 marks)

10) Analyze how does the cybercrimes related to the extended enterprise context? (8 marks)

11) Compare i)Email Spoofing ii)Hacking iii)Salami Attack iv)Software Piracy v)Computer Sabotage. (10 marks)

MODULE-5

1) List out the stages of an attack used to compromise a network. (8 marks)
2) What is Antikeylogger? (2 marks)
3) Differentiate proxy servers and anonymizers. (5 marks)
4) Explain the working of phishing. (5 marks)
5) Differentiate online and offline attacks. (5 marks)
6) Discuss the general guidelines for password policies. (8 marks)
7) Discuss the password guidelines for netizens. (8marks)
8) Differentiate Keyloggers and spywares. (5 marks)
9) Differentiate viruses and worms. (5 marks)
10) With a neat sketch, explain how does a virus spread through internet. (8 marks)
11) Explain the different types of viruses. (8 marks)
12) List out the various levels of DoS attacks. (8 marks)
13) Explain the different traditional techniques of Attacks on Wireless Networks. (8 marks)
14) List out the different ways to secure wireless networks? (5 marks)
15) What is MIMT? (2 marks)
16) Differentiate between Trojan horses and backdoors. (5 marks)
17) What is steganography? (2 marks)
18) What is Keylogger? Explain the types of Keyloggers. (8 marks)
19) List out some functions of Backdoor. (8 marks)
20) With a neat sketch, explain how does a virus spread through stand-alone system. (8 marks)
21) With a neat sketch, explain how does a virus spread through the network. (8 marks)
22) List and explain the different malware. (8 marks)
23) Differentiate between steganography and cryptography. (2 marks)
24) List out the various protection measures from DoS/DDoS Attacks. (8 marks)
25) What are the different tools used in DoS attack? (2 marks)
26) What are the types of Mobile workers? (2 marks)
27) Mention any tools used for hacking wireless networks. (2 marks)
28) List out the different steps to Secure the Wireless Networks. (8 marks)
29) Explain phishing. (5 marks)
30) Explain the various methods of phishing? (8 marks)
31) Differentiate spear phishing and whaling. (5 marks)
32) Explain the various phishing techniques. (8 marks)
33) What is distributed phishing? (2 marks)
34) What do you mean by spear phishing? (2 marks)
35) Explain the three P’s of cybercrime. (6 marks)
36) What is DNS hijacking. (2 marks)
37) Explain the various types of phishing scams. (12 marks)
38) Explain the steps to be adopted for not falling as a victim of phishing attack. (12 marks)
39) Explain the various countermeasures associated with phishing. (12 marks)
40) What are Honeypots? With the neat diagram Explain the Honeypots. (8 marks)
41) What is Intrusion Detection System? (2 marks)
42) What is identity theft? (2 marks)
43) What is PII? (2 marks)
44) Differentiate the seven various types of identity theft. (8 marks)
45) List out the different techniques involved in identity theft. (10 marks)
46) Explain the broad class of intruders and the classes based on skill level. (8 marks)
47) Explain the various countermeasures associated with Identity Theft. (8 marks)