CHHATRAPATI SHIVAJI INSTITUTE OF TECHNOLOGY, DURG
DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING

QUESTION BANK

UNIT-1

1. Use the additive cipher with key 15 to encrypt the message “Welcome”.
2. Using Caesar cipher formula with key=3, encrypt the following message.
   “ATTACK ON YOUR ENEMY”
3. Define Cryptanalysis?
4. Explain message Encryption? Discuss the different techniques of encrypting a message?
5. List the various types of security attacks in cryptography?
6. What are the essential in gradients of a symmetric cipher?
7. What are the two basic functions used in encryption algorithms?
8. How many keys are required for two people to communicate via a cipher?
9. What is the difference between a block cipher & a stream cipher?
10. What are the two general approaches to attacking a cipher?
11. List & briefly define types of cryptanalytic attacks based on what is known to the attacker?
12. Construct a play fair matrix with the key largest?
13. Construct a play fair matrix with the key occurrence. Make a reasonable assumption about how to treat redundant letters in the key?
14. Using this play fair matrix

M	F	H	I/J	K
U	N	O	P	Q
Z	V	W	X	Y
E	L	A	R	G
D	S	T	B	C

Encrypt this message:-

Must see you over cadogan west. Coming at once.

(Note: - The message is from the Sherlock Holmes story, the adventure of the Bruce parting ton plans.)

15. Explain DES (Data Encryption Algorithm) in detail. Write the difference between DES & TDES (Triple Data Encryption Algorithm)?
16. Write short notes on: (any two)
    (i) Transposition technique.
    (ii) Diffusion & Confusion.
    (iii) Cipher block chaining mode.
17. Describe the play fair cipher matrix making and encryption rules, using “play fair example” as the key and encrypting message “How are you”?
18. Draw the extended Euclid’s process model & also write the algorithm with an appropriate example?
19. Describe the DES (Data Encryption Algorithm) scheme and also the working of each block associated with it?
20. Determine the GCD of the following pairs of polynomials using Euclidian algorithm.
    (x^3+x+1) and (x^x+x+1) over GF(2).

21. Define finite field of order ‘P’, GF (P) and construct the following tables.
    (i) Addition module 8
    (ii) Multiplication module 8
    (iii) Additive & Multiplicative inverse module 8.
22. Explain the different modes of operation in cryptography.

QUESTION BANK

UNIT-2

1. What is the difference between a block cipher and a stream cipher & give an example of each?
2. Discuss Encryption & Decryption of Blowfish algorithm with neat diagram?
3. Explain about cryptographically generated Random numbers?
4. Discuss RC 4 algorithm in detail?
5. If the next byte generated by the generator is “01101100” & the next plaintext byte is “11001100” then the resulting cipher text byte is?
6. What is the basic criteria of AES evaluation & also discussed the round Structure of AES?
7. Show that the single round structure of Blowfish & explain its working?
8. Discuss the RC 5 characteristics and key generation technique?
9. Draw the IDEA (“International Data Encryption Algorithm”) rounds structure & explain in detail?
10. What common mathematical constants are used in RC 5?
11. Explain the Blowfish Encryption algorithm?
12. Describe the stream cipher. Discuss RC 4 algorithm with its characteristics?
13. Write in detail about:-
    (i) Pseudo random sequence,
    (ii) Linear congruential generators.

CHHATRAPATI SHIVAJI INSTITUTE OF TECHNOLOGY, DURG
DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING

QUESTION BANK

UNIT-3

1. What basic arithmetic & logical functions are used in MD5?
2. Find the value of phi-function Φ (240).
3. Define Euler's Totient Function and find the value of Φ (21).
4. Find the digest bits for input pattern, "7230248019".
5. Perform encryption & Decryption using RSA algorithm.
   (i) P=7 ; q=11 , e=17 ;m=8
   (ii) P=11 ; q=13 ,e=11 ;m=7.
6. Write the difference between conventional encryption & public key encryption?
7. Explain in detail about RIPEMD-160 digest algorithm with its advantages.
8. Compare the Diffie-Hellman Key exchange algorithm with Bucket-Bridge Problem.
9. Write the RSA algorithm ,and if two prime numbers are p=17 and q=11,so find the value of public key and private key according to RSA algorithmic logic.
10. Give the overview ,about the working of MD-5.
11. Explain the need of public key cryptography and the requirements to achieve it.
12. Describe Diffie-Hellman algorithm.
13. Explain in detail HMAC structure with neat diagram.
14. Explain the round structure of "Message Digest 5" with proper logical unit for each round.
15. Describe the Bucket Bridge Attack with respect to Diffie-Hellman Key Exchange Algorithm.
16. Explain the need of public-key cryptography and the requirements to achieve it.

CHHATRAPATI SHIVAJI INSTITUTE OF TECHNOLOGY, DURG
DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING

QUESTION BANK

UNIT-4

1. Define Network security.
2. Define the term IP security.
3. Differentiate between Transport mode and Tunnel mode for Authentication Header (AH).
4. In which layer of OSI protocol, Secure Socket Layer(SSL) is used.
5. Explain the operational description of PGP(Pretty Good Privacy)?
6. Write short notes on :
   (i) MIME
   (ii) SSL & TLS (Secure socket & Transport Layer)
7. Write the requirements & properties of a digital signature?
8. Explain all the exchanges involved in authentication using ‘KERBEROS’ protocol.
9. Describe DSS (Digital Signature Standard) and DSA (Digital Signature Algorithm) techniques.
10. Give the operational description of PGP (Pretty Good Privacy). Discuss the types of keys used by PGP.
11. Explain SSL (Secure Sockets Layer) and TSL (Transport Layer Security) Architecture with suitable diagrams.
12. Give the Kerberos version 4 message exchanges for the request for service in another Realm with neat diagram.
13. Draw IPSec ESP format and explain each field in it.
14. Compare SSL and TLS.
15. Explain all the release updates involved in authentication using KERBEROS protocol.
16. How many types of services are included in PGP (Pretty Good Privacy)? Discuss in detail.
17. Draft the IPSec Architecture, describing its components.

CHHATRAPATI SHIVAJI INSTITUTE OF TECHNOLOGY, DURG
DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING

QUESTION BANK

UNIT-5

1. Define Virus?
2. Define the term Hardened Firewall.
3. List out the four phases of virus, during its life time.
4. Define the term Secure Electronic Transaction.
5. Define the term DigiCash.
6. Define Smart Card Based System.
7. Explain firewall & types of firewall?
8. Write down the typical phases of operation of a virus or worm.
9. Write short notes on:
   (i) Secure Electronic Transaction (SET)
   (ii) Smart Card Based System
10. Write the classification of viruses. Explain with the help of diagram, actions and uses of firewall.
11. Explain Electronic Payment Systems with an appropriate example.
12. Explain various classes of Intruders, and also discuss about the type of Intrusion techniques.
13. Explain how merchant verifies customer purchase request in Secure Electronic Transaction (SET).
14. Discuss Trojan Horse Defense with the help of diagram.
15. What is a firewall? Give the capabilities and limitations of Firewall.
16. What are the various modes of electronic payments?
17. Explain various classes of intruders. Discuss about the type of intrusion techniques.
18. What is a Firewall? Explain with the help of diagram, actions and uses of Firewall.