BHARTIYA INSTITUTE OF ENGINEERING TECHNOLOGY, SIKAR

DEPARTMENT OF COMPUTER ENGINEERING

III YEAR VI SEMESTER

INFORMATION SYSTEM SECURITY

UNIT-1

Short type question:

1. What is cryptography and cryptanalysis?
2. Explain Cryptology.
3. Difference between plain text and cipher text.
4. Difference between Encryption and Decryption.
5. What is symmetric key and Asymmetric key Cryptography.

Long type question:

1. List the mechanisms employed to the following attacks:
   - i) Released of message content
   - ii) Traffic analysis
   - iii) Masquerade
   - iv) Reply
   - v) Modification of messages
   - vi) Denial of services

   Also explain each attack.
2. Explain the difference between Stream cipher and Block cipher.
3. Explain the substitution techniques and transposition techniques in brief.
4. Explain the mechanism of security.
5. How can Caesar Cipher be cracked. And How it is different from monoalphabetic Cipher.

UNIT-2

Short type question:

1. What is an Initilization Vector?What is its Significance?
2. What are the problems with Symmetric key encryption?
3. What are the Block cipher modes.
4. What is the difference AES and DES.

Long type question:

1. Explain all block cipher modes of operation with diagram.

2. Explain the parameters and design choices determines real algorithm of Feistel cipher? 3. Explain Feistel decryption algorithm.

4. Describe the DES algorithm in detail.

5. What is AES? What Are the major parameters used in AES? Explain the processing of plaintext with a suitable example.

6. Explain triple DES.How can the same key be reused in triple DES?

BHARTIYA INSTITUTE OF ENGINEERING & TECHNOLOGY, SIKAR

Department of Computer Science Engineering

ISS(Question Bank)

Unit-3

Short type Question:

1.What is the mean by ELGAMAL cryptosystem?
2. Write the applications of public key cryptosystem.
3.Define Cryptanalysis.
4.Define trap door function.
5.define key and plain text.

Long type Question:

1. Explain the working of public key cryptosystem.
2. Define Elliptic curve cryptosystem.Explain with example.
3. Explain RSA cryptosystem with mathematic example.
4. What are the requirements of public key cryptosystem.
5. What are the requirements for the use of a public key certificate scheme?

Unit-4

Short type Question:

1.What is mean by one way property in Hash function?
2. What is Hash function?
3.What is the difference between a message authentication code and a one way hash function.
4.What is meant by the function of a compression function in a hash function?
5.How Hash function are different from public key cryptography and secret key cryptography.
6. Define digital signatutre.
7.Write the four SSL protocols.

Long type Question:

1. What is message authentication code.Explain tpes of MAC.
2. Why is message authentication required?Explain various authentication protocol.
3. What is Digital Signature.Show how signing and verification is done using digital signature standard.
4. Explain Elagmal signatures and undeniable signatures.
5. Differentiate between MAC and Hash value.What are the characteristics of a good hash function?

Unit-5

Short type Question:

1.List out the requirement of KERBEROS.
2.Define transport layer security.
3.Differentiate between HTTPS and SSL.
4.Define public key directory.
5.Difference between public key authority and certificate authority.

Long type Question:

1. What is X.509 certificate? Differentiate between X.509 client certificate and a normal SSL certidicate.
2. Explain X.509 certificate and what role certificate authority play in it.
3. Explain Kerberos concept in detail.
4. Explain public key infrastructure in detail.
5.Explain SSL architecture in detail.
6.Write short note on:
   a) Distribution of Public key .
   b) Distribution of Secret key using public key cryptosystem.