SRI VIDYA COLLEGE OF ENGINEERING & TECHNOLOGY

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

QUESTION BANK

Year / Dept / Sem: IV / CSE / 07 **Subject code: CS6551**

Staff Name : M.Mohana **SubjectName: Cryptography and Network Security**

UNIT-II

PART-A

1. **Compare stream cipher with block cipher with example.**

Stream cipher: Processes the input stream continuously and producing one element at a time. **Example: caeser cipher**.

Block cipher: Processes the input one block of elements at a time producing an output block for each input block. **Example: DES.**

2. **Differentiate unconditionally secured and computationally secured .**

An Encryption algorithm is unconditionally secured means, the condition is if the cipher text generated by the encryption scheme doesn’t contain enough information to determine corresponding plaintext.

Encryption is computationally secured means,

1. The cost of breaking the cipher exceed the value of enough information.
2. Time required to break the cipher exceed the useful lifetime of information.

3. **Define Diffusion & Cnfusion.**

Diffusion:

It means each plaintext digits affect the values of many ciphertext digits which is equivalent to each ciphertext digit is affected by many plaintext digits. It can be achieved by performing permutation on the data. It is the relationship between the plaintext and ciphertext.

Confusion:

It can be achieved by substitution algorithm. It is the relationship between cipher text and key.

4. **What are the design parameters of Feistel cipher network?**

*Block size
*Key size
*Number of Rounds
*Sub key generation algorithm
*Round function
*Fast software Encryption/Decryption
*Ease of analysis

5. **Define Product cipher.**

It means two or more basic cipher are combined and it produce the resultant cipher is called the product cipher.

6. **Explain Avalanche effect.**

A desirable property of any encryption algorithm is that a small change in either the plaintext or the key produce a significant change in the ciphertext. In particular, a change in one bit of the plaintext or one bit of the key should produce a change in manybits of the ciphertext. If the change is small, this might provider a way to reduce the size of the plaintext or key space to be searched.

7. Give the five modes of operation of Block cipher.

i. Electronic Codebook(ECB)
ii. Cipher Block Chaining(CBC)
iii. Cipher Feedback(CFB)
iv. Output Feedback(OFB)
v. Counter(CTR)

8. State advantages of counter mode.

*Hardware Efficiency * Software Efficiency

*Preprocessing * Random Access

* Provable Security * Simplicity.

9. Define Multiple Encryption.

It is a technique in which the encryption is used multiple times. Eg: Double DES, Triple DES

10. Specify the design criteria of block cipher.

- Number of rounds
- Design of the function F
- Key scheduling

11. Define Reversible mapping.

Each plain text is maps with the unique cipher text. This transformation is called reversible mapping.

12. Specify the basic task for defining a security service.

A service that enhances the security of the data processing systems and the information transfer of an organization. The services are intended to counter security attack, and they make use of one or more security mechanism to provide the service.

13. What is the difference between link and end to end encryption?

Link Encryption	**End to End Encryption**
1.With link encryption, each vulnerable communication link is equipped on Both ends with an encryption device	1.With end to end ncryption, encryption process is carried out at the two end systems
2.Message exposed in sending host and in intermediate nodes	2.Message encrypted in sending and intermediate nodes
3.Transperant to user	3.User applies encryption
4.Host maintains encryption facility	4.Users must determine algorithm
5.One facility for all users	5.Users selects encryption scheme
6.Can be done in hardware	6.Software implementations
7.Provides host authentication	7.Provides user authentication
8.Requires one key per(host-intermediate) Pair and (intermediate-intermediate) pair	8.Requires one key per user pair

14. What is traffic Padding? What is its purpose?

Traffic padding produces ciphertext output continuously, even in the absence of the plain text. A continuous random data stream is generated. When plain text is available, it is encrypted and transmitted. When input plaintext is not present, random data are encrypted and transmitted. This makes it impossible to for an attacker to distinguish between true dataflow and padding and therefore impossible to deduce the amount of traffic.

15. List the evaluation criteria defined by NIST for AES?

The evaluation criteria for AES is as follows:

1.Security
2. Cost
3.Algorithm and implementation characteristics

16. What is Triple Encryption? How many keys are used in triple encryption?

Triple Encryption is a technique in which encryption algorithm is performed three times using three keys.

17. List the schemes for the distribution of public keys.

- Public announcement
- Publicly available directory
- Public key authority
- Public-key certificates

18. Drawback of 3-DES.

- Algorithm is sluggish in software
- The number of rounds in thrice as that of DES
- 3DES uses 64 bit block size
- To have higher efficiency and security a larger block size is needed.

19. List out an evaluation criteria for round 2.

- General security
- Software implementation
- Hardware implementation
- Attacks
- Encryption Vs Decryption
- Key ability-Ability to change keys quickly with minimum of resources.
- Versatility and Flexibility
- Instruction level parallelism.

20. List out the attacks to RSA.

- **Brute force** - Trying all possible private keys.
- **Mathematical attacks** - The approaches to factor the product of two prime numbers.
- **Timing attack** - Depends on the running time of the decryption algorithm.

PART-B

1.State and explain the principles of public key cryptography?
2.Explain Diffie Hellman key Exchange in detail with an example?
3.Explain the key management of public key encryption in detail?
4.Explain RSA algorithm in detail with an example?
5.Briefly explain the idea behind Elliptic Curve Cryptosystem?
6.Explain Data Encryption Standard (DES) in detail. (16)
How AES is used for encryption/decryption? Discuss with example. (16)
7.List the evaluation criteria defined by NIST for AES. (16)
8.Using play fair cipher algorithm encrypts the message using the key "MONARCHY" and Explains the poly alphabetic key. (16)
9.Explain 1.ceaser cipher 2. Mono alphabetic cipher 3.one time pad cipher (16)
10.Explain the Key Generation, Encryption and Decryption of DES algorithm in detail. (16)

11.Explain in detail the key generation in AES algorithm and its expansion format. (16)
12.a. Explain single round DES with neat sketch.(10)
b .Explain Double &Triple DES with keys. (6)
13. Explain the block cipher modes of operation. (16)
14.Explain the key management of public key encryption in detail. (16)
15.Explain ECC - Diffie Hellman key Exchange with both keys in detail with an example. (16)
16.Write about elliptic curve architecture in detail and how they are useful for cryptography. (16)
17.a. Write about key distribution in detail. (10)
b. Explain the purpose of CRT. (6)
18.Explain the different methods used in random number generation. (16)
19. What are the requirements and applications of public key? Compare conventional with public key
encryption. (16)
20.(i) Identify the possible threats for RSA algorithm and list their counter measures. (8)
(ii) Perform decryption and encryption using RSA algorithm with p=3, q=11, e=7 and N=5. (8)
21. (i) Draw the general structure of DES and explain the encryption decryption process. (10)
(ii) Mention the strengths and weakness of DES algorithm. (6)
22. (i) Explain the generation sub key and S Box from the given 32-bit key by
Blowfish. (8)
(ii) In AES, hoe the encryption key is expanded to produce keys for the 10 rounds.(8)
23.(i) Describe about RC4 algorithm. (8)
(ii) Explain the Miller-Rabin algorithm. (8)