UNIT 2- 2 MARKS

1. **What is the difference between a block cipher and a stream cipher?**
   A *block cipher* processes the input one block of elements at a time, producing an output block for each input block. A *stream cipher* processes the input elements continuously, producing output one element at a time, as it goes along.
2. **What is the difference between diffusion and confusion?**
   In **diffusion**, the statistical structure of the plaintext is dissipated into long-range statistics of the ciphertext. This is achieved by having each plaintext digit affect the value of many ciphertext digits; generally, this is equivalent to having each ciphertext digit be affected by many plaintext digits. **confusion** seeks to make the relationship between the statistics of the ciphertext and the value of the encryption key as complex as possible, again to thwart attempts to discover the key. Thus, even if the attacker can get some handle on the statistics of the ciphertext, the way in which the key was used to produce that ciphertext is so complex as to make it difficult to deduce the key.This is achieved by the use of a complex substitution algorithm.
3. **Whar are the design parameters of a Feistel cipher?**
   - Block size
   - Key size
   - Number of rounds
   - Subkey generation algorithm
   - Round function F
   - Fast software encryption/ Decryption
   - Ease of analysis
4. **Explain the avalanche effect.**
   A desirable property of any encryption algorithm is that a small change in either the plaintext or the key should 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 many bits of the ciphertext. This is referred to as the avalanche effect. If the change were small, this might provide a way to reduce the size of the plaintext or key space to be searched.
5. **What is the strength of DES?**
   - The use of 56 bit keys
   - The nature of DES algorithm
   - Timing attacks
6. **Define product cipher**
   product cipher, which is the execution of two or more simple ciphers in sequence in such a way that the final result or product is cryptographically stronger than any of the component ciphers.
7. **What is substitution and permutation?**
   Substitution: Each plaintext element or group of elements is uniquely replaced by a corresponding ciphertext element or group of elements.
   Permutation: A sequence of plaintext elements is replaced by a permutation of that sequence. That is, no elements are added or deleted or replaced in the sequence, rather the order in which the elements appear in the sequence is changed.
8. **Give 5 modes of operation in block cipher**
   - Electronic Codebook(ECB)
   - Cipher Block Chaining(CBC)

- Cipher Feedback(CFB)
- Output Feedback(OFB)
- Counter(CTR)

9. **State advantages of counter mode.**
   *Hardware Efficiency
   * Software Efficiency
   *Preprocessing
   * Random Access
   * Provable Security
   * Simplicity.
10. **Define Multiple Encryption.**
    It is a technique in which the encryption is used multiple times. Eg: Double DES, Triple DES. In the first instance, plaintext is converted to ciphertext using the encryption algorithm. This ciphertext is then used as input and the algorithm is applied again. This process may be repeated through any number of stages.
11. **Specify the design criteria of block cipher.**
    - Number of rounds
    - Design of the function F
    - Key scheduling
12. **Define Reversible mapping.**
    Each plain text is maps with the unique cipher text. This transformation is called reversible mapping.
13. **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.
14. **List the schemes for the distribution of public keys.**
    - Public announcement
    - Publicly available directory
    - Public key authority
    - Public-key certificates
15. **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.
16. **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.

17. **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.
18. **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

19. Table 9.2 Conventional and Public-Key Encryption

Conventional Encryption	Public-Key Encryption
Needed to Work: 1. The same algorithm with the same key is used for encryption and decryption. 2. The sender and receiver must share the algorithm and the key. *Needed for Security:* 1. The key must be kept secret. 2. It must be impossible or at least impractical to decipher a message if no other information is available. 3. Knowledge of the algorithm plus samples of ciphertext must be insufficient to determine the key.	*Needed to Work:* 1. One algorithm is used for encryption and decryption with a pair of keys, one for encryption and one for decryption. 2. The sender and receiver must each have one of the matched pair of keys (not the same one). *Needed for Security:* 1. One of the two keys must be kept secret. 2. It must be impossible or at least impractical to decipher a message if no other information is available. 3. Knowledge of the algorithm plus one of the keys plus samples of ciphertext must be insufficient to determine the other key.

20. **What is one way function?**

A **one-way function**3 is one that maps a domain into a range such that every function value has a unique inverse, with the condition that the calculation of the function is easy, whereas the calculation of the inverse is infeasible:

$Y = f(X)$ easy

$X = f^{-1}(Y)$ infeasible

21. **What is a trap-door one-way function?**

a **trap-door one-way function**, which is easy to calculate in one direction and infeasible to calculate in the other direction unless certain additional information is known. With the additional information the inverse can be calculated in polynomial time.We can summarize as follows: A trapdoor one-way function is a family of invertible functions f_k, such that

$Y = f_k(X)$ easy, if k and X are known

$X = f_k^{-1}(Y)$ easy, if k and Y are known

$X = f_k^{-1}(Y)$ infeasible, if Y is known but k is not known

22. **Formulate few applications of RC5**

23. **List the parameters(block size, key size, and no.of rounds) for the three AES version**

Key size(words/bytes/bit)	**4/16/128**	**6/24/192**	**8/32/256**
Plaintext Block size(words/bytes/bit)	**4/16/128**	**4/16/128**	**4/16/128**
Number of rounds	**10**	**12**	**14**
Round key size(words/bytes/bit)	**4/16/128**	**4/16/128**	**4/16/128**
Expanded key size (words/bytes)	**44/176**	**52/208**	**60/240**

15 MARKS

1. **Explain in detail about working of DES encryption and decryption**
   - Definition
   - Encryption- Diagram
   - Initial Permutation
   - Details of Single Round- diagram , S-box
   - decryption
2. **Explain in detail about working of AES**
   Definition
   Structure – diagram and its explanation (10 pt)
   Transformation function
3. **Explain in detail about AES key expansion**
4. **Explain briefly about the block cipher modes of operations**
   Diagram , adv and disadv for each
   - Electronic Codebook(ECB)
   - Cipher Block Chaining(CBC)
   - Cipher Feedback(CFB)
   - Output Feedback(OFB)
   - Counter(CTR)
5. **Perform encryption and decryption using the RSA algorithm, as in Figure 9.5, for the following:**
   a. $p = 3; q = 11, e = 7; M = 5$
   b. $p = 5; q = 11, e = 3; M = 9$
   c. $p = 7; q = 11, e = 17; M = 8$
   d. $p = 11; q = 13, e = 11; M = 7$
   e. $p = 17; q = 31, e = 7; M = 2$

5. In a public-key system using RSA, you intercept the ciphertext $C = 10$ sent to a user whose public key is $e = 5$, $n = 35$. What is the plaintext M?

6. Users A and B use the Diffie-Hellman key exchange technique with a common prime q=71 and a primitive root $\alpha=7$.

a. If user A has private key $X_a = 5$, what is A's public key Y_a ?
b. If user B has private key $X_b=12$, what is B's public key Y_b ?
c. What is the shared secret key?

7. Consider a Diffie-Hellman scheme with a common prime q=11 and a primitive root $\alpha=2$

a. Show that 2 is a primitive root of 11.
b. If user A has public key $Y_a = 9$, what is A's private key X_a?
c. If user B has public key $Y_b = 3$, what is the secret key K shared with A?

8. Evaluate using Diffie-Hellman key exchange technique. Users A and B use a common prime q=11 and a primitive root alpha=7. (16)
(i) If user A has private key XA=3.What is A's public key YA?
(ii)If user B has private key XB=6. What is B's public key YB?
(iii) What is the shared secret key? Also write the algorithm.

9. Explain in detail about RC5 algorithm

10. Brief about Blowfish algorithm