Unit-1 Two marks

<table>
<tr><th>S. No.</th><th>Question</th></tr>
<tr><td>1</td><td><b>Differentiate passive attack from active attack with example. (</b>
<table>
<tr><th>Passive Attack</th><th>Active Attack</th></tr>
<tr><td>1. Passive attacks do not affect system resources
• Eavesdropping, monitoring
2. Two types of passive attacks
• Releasof message
• Traffic analysis
3. Passive attacks are very difficult to detect</td><td>1. Active attacks try to alter system resources or affect their operation
• Modification of data, or creation of false data
2. Four categories
• Masquerade
• Replay
• Modification of messages
• Denial of service: preventing normal use
<b>3.</b> Difficult to prevent</td></tr>
</table></td></tr>
<tr><td>2</td><td><b>What are the 3 aspects of security?</b>
• Security Attack
• Security Mechanism
• Security Service</td></tr>
<tr><td>3</td><td><b>Define Security attacks.</b>
Security attack: Any action that compromises the security of information owned by an organization.</td></tr>
<tr><td>4</td><td><b>Define security mechanism.</b>
Security mechanism: A process that is designed to detect, prevent, or recover from a security attack</td></tr>
<tr><td><b>5</b></td><td><b>Define Security service.</b>
<b>A processing or communication service that enhances the security of the data processing systems and the information transfers of an organization. The services are intended to counter security attacks, and they make use of one or more security mechanisms to provide the service.</b></td></tr>
<tr><td><b>6</b></td><td><b>Define cryptanalysis?</b>
<b>The study of principles and methods of transforming an unintelligible message back into an intelligible message without the knowledge of the key. It is also called code breaking.</b></td></tr>
</table>

7	**Define Steganography** **It is the process of hiding the message into some cover media. It hides the existence of a message. Ex: Character marking, Pin punctures, Invisible ink etc**
8	**What are the two basic functions used in encryption algorithms?** **The two basic functions used in encryption algorithms are** • **Substitution** • **Transposition**
9	**Define Threat and attack. (NOV2009)** **Threat is a possible danger that might exploit a vulnerability to breach security and thus cause possible harm.** **Attack is any attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an asset**
10	**What are the two approaches to attacking a cipher?** **The two approaches to attack a cipher are:** **1.Cryptanalysis 2.Brute-force attack**
11	**Define Brute-force attack.** **The attacker tries every possible key on a piece of cipher text until an intelligible translation into plaintext is obtained. On average, half of all possible keys must be tried to achieve success.**
12	**What is Modification of messages** **Modification of messages simply means that some portion of a**
	legitimate message is altered, or that messages are delayed or reordered, to produce an unauthorized effect.
13	**What is masquerade?** **A masquerade takes place when one entity pretends to be a different entity. For example, authentication sequences can be captured and replayed after a valid authentication sequence has taken place, thus enabling an authorized entity with few privileges to obtain extra privileges by impersonating an entity that has those privileges**
14	**What is Replay?** **Replay involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect.**
15	**Define Denial of service.** **Prevents or inhibits the normal use or management of communication facilities. Another form of service denial is the disruption of an entire network, either by disabling the network or overloading it with messages so as to degrade performance**
16	**List out the components of encryption algorithm.** 1. **Plaintext** 2. **Encryption algorithm**

	3. **Secret key** 4. **Cipher text** 5. **Decryption algorithm**
17	**Compare Substitution and Transposition techniques.** **Substitution techniques: A substitution techniques is one in which the letters of plaintext are replaced by other letter or by number or symbols. Ex: Caeser cipher.** **Transposition techniques: It process in which different kind of mapping is achieved by performing some sort of permutation on the plaintext letterset. Ex: DES, AES.**
18	**Specify the four categories of security threads?** - **Interruption** - **Interception** - **Modification**
	- **Fabrication**
19	**Define integrity.** **It assures that the data received is sent by an authorized entity and are not modified/replayed/deleted/updated**
20	**Define Non repudiation.** **It is the process which protects against denial by one of the parties in a communication. It can be obtained through the use of digital signature, time stamps etc,.**
21	**Differentiate symmetric and asymmetric encryption?** **Symmetric: It is a form of cryptosystem in which encryption and decryption performed using the same key.** **Asymmetric: It is a form of cryptosystem in which encryption and decryption performed using two keys. Eg: DES, AES Eg: RSA, ECC**
22	**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.**
23	**Convert the Given Text “CRYPTOGRAPHY” into cipher text using Rail fence Technique.** **In rail fence technique the plaintext is written down as a sequence of diagonals and then read off as a sequence of rows.** **C Y T G A H R P O R P Y** **The cipher text is CYTGAH RPORPY.**
S. No.	**Question**

Unit-1 Two marks

1	What are the different modes of operation in DES? (APR 2011 , APR 2017) Electronic Code Book (ECB) Cipher Block Chaining (CBC) Cipher Feedback (CFB) Output Feedback (OFB) Counter Mode
2	Write down the purpose of S-Boxes in DES? (NOV 2011) Each row of a S-box defines a general reversible substitution. It consists of a set of eight S-boxes, each of which accepts 6 bits as input and produces 4 bits as output.
3	What is the difference between diffusion and confusion?(NOV 2011) In diffusion, the statistical structure of the plain text is dissipated into long-range statistics of the cipher text. This is achieved by permutation. In confusion, the relationship between the statistics of the cipher text and the value of the encryption key is made complex. It is achieved by substitution
4	What is the difference between differential and linear cryptanalysis?(APR 2012) Differential cryptanalysis is the first published attack that
	is capable of breaking DES in less than encryptions. Linear Cryptanalysis method can find a DES key given known 243plaintexts, as compared to247chosen plaintexts for differential cryptanalysis
5	What are disadvantages of double DES? (NOV 2012) Reduction to a single stage. Meet in the middle attacks.
6	What is an avalanche effect? (NOV 2012) It is that a small change in either the plaintext or the key should produce a significant change in the cipher text.A change in one of the bit of the plaintext or one bit of the key should produce a change in many bits of the cipher text
7	Define product cipher. Product cipher performs two or more basic ciphers in sequence in such a way that the final result or product is crypto logically stronger than any of the component ciphers.
8	What is a meet-in-the-middle attack? Meet-in-the-middle attack was first described in [DIFF77]. It is based on the observation that, if we have C=Ek2[Ek1[P]] Then X=Ek1[P]=Dk2[C] Given a known pair, (P,C), the attack proceeds as follows. First, encrypt P for all 256 possible values of K1. Store these results in a table and then sort the table by the values of X. Next, decrypt C using all 256 possible values of K2. As each decryption is produced, check the result against the table for a match. If a match occurs, then test the two resulting keys against a new known plaintext-

	cipher textpair. If the two keys produce the correct cipher text, accept them as the correct keys.		
9	**Brief the strength of triple DES. (DEC 2016)** It is a reuse DES implementation by cascading three instances of DES. It is believed to be secure up to at least security	C401.2	BTL 1