

① Passive & Active attack:	Activ attack
<u>Passive attack</u> Passive attacks are in the nature of eavesdropping on or monitoring of transmissions	<u>Activ attack</u> Active Attacks involve some modification of the data stream or the creation of a false stream
Types: Release of message contents and traffic analysis	Types: Masquerade, replay, modification of message and denial of service
The emphasis in dealing with passive attacks is on prevention rather than detection	It is quite difficult to prevent active attacks absolutely
Very difficult to detect	Easy to detect
It does not affect the system	It affects the system
Q) What do you mean by Cryptanalysis:	Techniques used for deciphering a message
without any knowledge of the enciphering details fall into the area of Cryptanalysis. Cryptanalysis is what the layperson calls "breaking the code".	The areas of cryptography and cryptanalysis together called Cryptology
Cryptanalytic attacks rely on the nature of the algorithm plus perhaps some knowledge of the general characteristics of the plaintext or even some sample plaintext cipher text pairs.	

③ List the two basic functions used in Encryption
algorithm.

All the encryption algorithm are based on
two general principle

• Substitution : In which the letters of plaintext
are replaced by other letters or by number or
symbols. The substitution techniques are

Caesar Cipher

Monoalphabetic Ciphers

Playfair Cipher

Hill Cipher

Polyalphabetic cipher

One-Time pad

Transposition : The process of rearranging the
letter in plaintext using key to form the
ciphertext is called Transpositional technique

classified into two types

• Rail fence

• Columnar transposition

④ Enumerate on Steganography

Steganography is the art and science
of writing hidden messages in such a way that
no one, apart from the sender and
intended recipient, suspects the existence
of the message a form of security through
obscenity.

Steganography : Conceal the existence of the
message, whereas the methods of cryptography
render message unintelligible to outsiders
by various transformation of the text.

$$\textcircled{6} \quad 117 \bmod 13$$

$$11^2 = 121 \equiv 4 \pmod{13}$$

$$11^4 = (11^2)^2 \equiv 4^2 \equiv 8 \pmod{13}$$

$$11^7 = 11 \times 4 \times$$

$$\textcircled{6} \quad \text{Gcd}(1970, 1066)$$

\textcircled{7} Block cipher & Stream

A stream cipher is one that encrypts a digital data stream on bit or one byte at a time. Examples of classical stream ciphers are the autokeyed Vigenere cipher and the Vernam cipher.

A block cipher is one in which a block of plaintext is treated as a whole and used to produce a ciphertext block of equal length. Typically a block size of 64 or 128 bits is used.

As with a stream cipher, the two users share a symmetric encryption key, it has broader range of application.

(diagrams)

11/8/2010

\textcircled{8} List out the parameters of AES
Key size, Plaintext Blocksize, Number of Rounds, Round key size, Expanded key size

\textcircled{9} What is the use of fermat's theorem?

① Fermat's theorem helps compute powers of integers modulo prime numbers

② It is helpful for quickly finding a square inverse if the modulus is a prime.

③ It is a specific case of Euler's theorem. It is essential in applications of elementary number theory like primality testing and public-key cry-

⑩ Euler's theorem states that for every and that are relatively prime $a^{\phi(n)} \equiv 1 \pmod{n}$

$\phi(n)$ is represented in Euler's totient function and defined as the number of positive integers less than n that are relatively prime to n . By convention $\phi(1) = 1$.

⑪ Differentiate active attacks & passive attacks

A passive attack attempts to learn or make use of information from the system but does not use system resources. Two types of passive attacks are the release of message contents and analysis.

A active attack attempts to alter system resources or effect their operation. It can be subdivided into four categories: masquerade, replay, modification of message and denial of service.

⑫ Define Cryptanalysis:

Technique used for deciphering a message without any knowledge of the enciphering details fall into the area of cryptanalysis. Cryptanalysis is what the lay person calls "breaking the codes".

⑬ Define Security Service

A processing or communication service that enhances the security of the data processing system's and the information transfer of an organization. The service are intended to counter security attacks and they make use of one or more security mechanisms to provide the service.

⑭ 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 sequence of rows.

C Y T G I A H R P O R P Y

The cipher text is C Y T G I A H R P O R P Y

$$\text{⑮ } \gcd(24140, 16762) \quad \gcd(a, b) = \gcd(b, a \bmod b)$$

$$\gcd(24140, 16762) = \gcd(16762, 24140 \bmod 16762)$$

$$= \gcd(16762, 7378) = \gcd(7378, 16762 \bmod 7378)$$

$$= \gcd(7378, 2006) = \gcd(2006, 7378 \bmod 2006)$$

$$= \gcd(2006, 1360) = \gcd(1360, 2006 \bmod 1360)$$

$$= \gcd(1360, 646) = \gcd(646, 1360 \bmod 646)$$

$$= \gcd(646, 68) = \gcd(68, 646 \bmod 68)$$

$$= \gcd(68, 34) = \gcd(34, 68 \bmod 34)$$

$$= \gcd(34, 0) = 34$$

16. Is it possible to use the DES algorithm to generate message authentication code? Justify
Yes, it can use any block cipher chaining mode and use final block as a MAC. Data Authentication Algorithm (DAA) is a widely used MAC based on DES-CBC Encrypt message using CBC mode and send just the final block as the MAC

Big question

- 1 ① OSI security Architecture
CSA, SS, SM Caeser, Monoalphabetic, Vigeneze, Playfair, Hillcipher
 - 1 ② Substitution techniques (Any 3) with example, Transposition techniques with example
 - 2 ③ DES algorithm
 - 2 ④ Advanced Encryption Standard
 - 3 ⑤ Fermat's & Euler's theorem
 - 2 ⑥ Diffie-Hellman key exchange Algorithm with Problem
 - 1 ⑦ Biometric and its Techniques
- 15 m
- $$q = 83 \quad d = 5$$
- $$g = 11 \quad a = 17 \quad b = 32 \quad GCD = (dPd, Qd) = 1$$
- $$(Gd, b^d) \bmod = (32^5, 11^5) \bmod = (18, 11) \bmod = 7$$
- $$NE = (a, PE) \bmod =$$