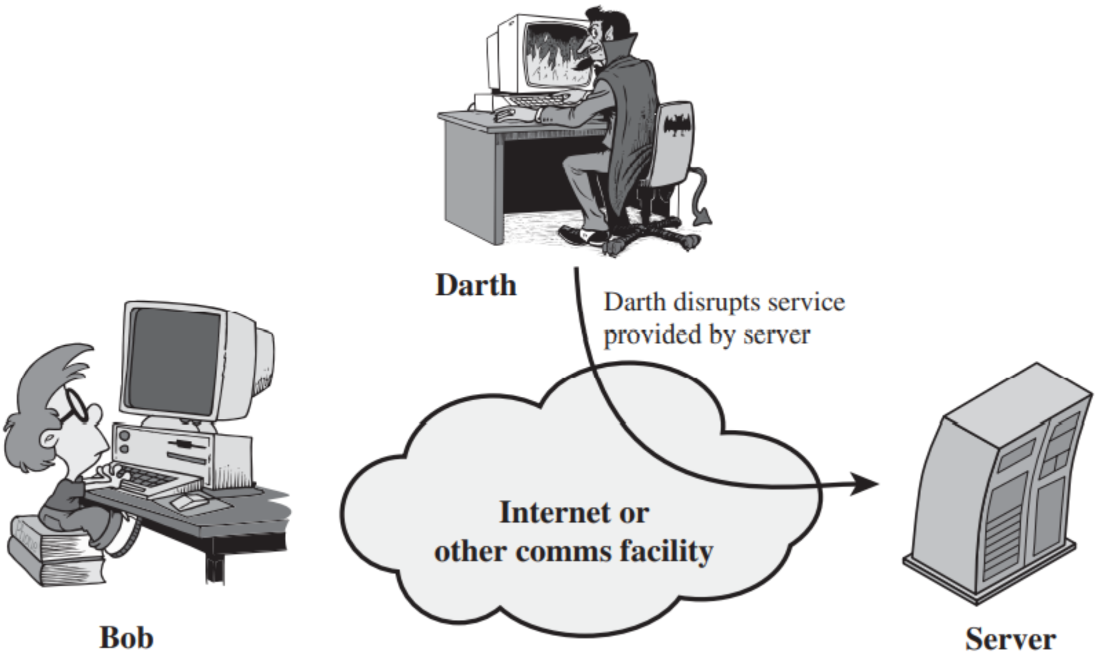
CS8792-CRYPTOGRAPHY AND NETWORK SECURITY

UNIT-I: INTRODUCTION

1.What is meant by Denial of Service [DoS]attack? Is it Active Attack or Passive Attack?[Nov/Dec 2021]

The **denial of service *<u>prevents or inhibits</u>*** the normal **use or management of communications facilities.**

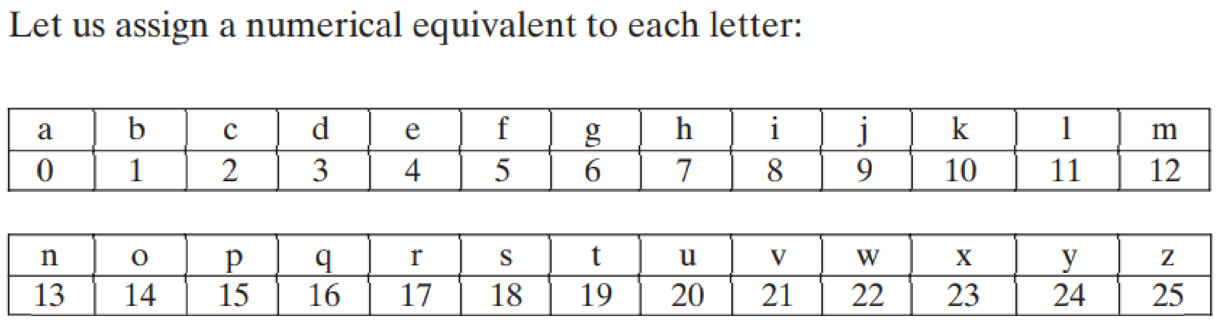
Example
An entity may suppress ***<u>all messages directed to a particular destination.</u>***


Darth
Darth disrupts service provided by server
Bob
Internet or other comms facility
Server

Denial of service

- It is an **Active Attack**
- Active attacks involve ***<u>some modification of the data stream or the creation of a false stream</u>*** and
- Denial of Service (DoS) can be category of **ActiveAttack**.

2. Let message = "Anna", and k = 3, find the ciphertext using Caesar.[Nov/Dec 2021]
Caesar algorithm
C = E (p,k) = (p+k) mod 26



Let us assign a numerical equivalent to each letter:

a	b	c	d	e	f	g	h	i	j	k	l	m
0	1	2	3	4	5	6	7	8	9	10	11	12

n	o	p	q	r	s	t	u	v	w	x	y	z
13	14	15	16	17	18	19	20	21	22	23	24	25

C=E(A,3)=(0+3)mod 26=d

C=E(N,3)=(13+3)mod 26=16 mod 26=q

Cipher text =dqqd

3.Differentiate active and passive attacks[Apr/May 2019]

On the basis of	Active Attack	Passive attack
Definition	In active attacks, the attacker intercepts the connection and efforts to modify the message's content.	In passive attacks, the attacker observes the messages, then copy and save them and can use it for malicious purposes.
Modification	In an active attack, the attacker modifies the actual information.	In passive attacks, information remains unchanged.
Types	Active attacks involve (i)Masquerade, (ii)Modification of message (iii) Replay (iv) Denial of service.	(i)Release of message contents (ii)traffic analysis
	Easy to detect	Difficult to detect

4.Specify the components of encryption algorithm[Apr/May 2019]

The main components of an encryption system are: \

(1) plaintext (not encrypted message), (2) encryption algorithm (works like a locking mechanism to a safe),

(3) key (works like the safe's combination), and

(4) ciphertext (produced from plaintext message by encryption key).

5.Distinguish between attack and threat?[Nov/Dec 2018]

Threat[2-marks]

A ***potential for violation of security***, because of

(1). Circumstances, (2). Capability, (3). Action or event that **break security** and **cause harm.** **Threat** is possible that might ***create Vulnerability***.

Attack[2-marks].

It is an intelligent act that is a deliberate attempt to
(1). **Avoid security services and (2). Violate the security policy of a system.**

6.Calculate the cipher text for the following using one time pad cipher(Perfect secrecy or Vernam Cipher)

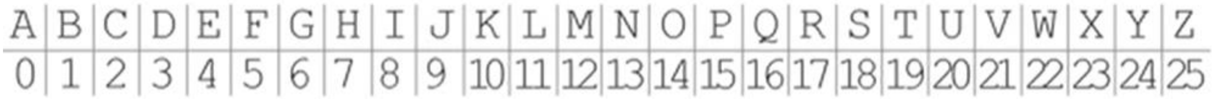
Plain Text:ROCK

Keyword:BOTS

Answer

Each **new message** requires **a new key of the same length** as the **new message**. Such a scheme, known as ***a one-time pad, is unbreakable***.

It produces **random output** that bears **no statistical *relationship*** to the **plaintext.**



A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Plain Text	R(17)	O(14)	C(2)	K(10)
Keyword	B(1)	O(14)	T(19)	S(18)
Sum (PT+K)	18	28	21	28
If Sum >25 then 26-sum	S	C(2)	V	C(2)

Cipher Text :SCVC

7.Define Brute-force attack.

The attacker tries every possible key on a piece of cipher text until an intelligible translation into plaintext is obtained.

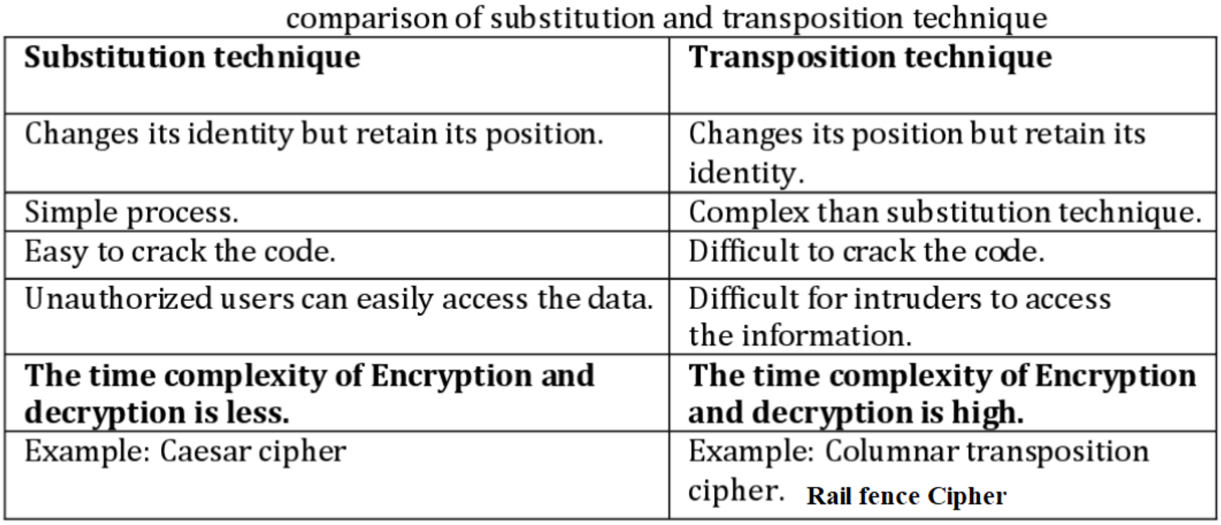
On average, half of all possible keys must be tried to achieve success

8.Give an example each for substitution and transposition ciphers.

Or

Define the two basic building blocks of encryption techniques

https://www.youtube.com/watch?v=OWeqP65Ixg8&list=PLzQqHxFtQGydze3lo22YC12IGfL0irVFs&index=15



comparison of substitution and transposition technique

Substitution technique	Transposition technique
Changes its identity but retain its position.	Changes its position but retain its identity.
Simple process.	Complex than substitution technique.
Easy to crack the code.	Difficult to crack the code.
Unauthorized users can easily access the data.	Difficult for intruders to access the information.
The time complexity of Encryption and decryption is less.	**The time complexity of Encryption and decryption is high.**
Example: Caesar cipher	Example: Columnar transposition cipher. **Rail fence Cipher**

9. List out the problems of one time pad?[Nov /Dec 2011]

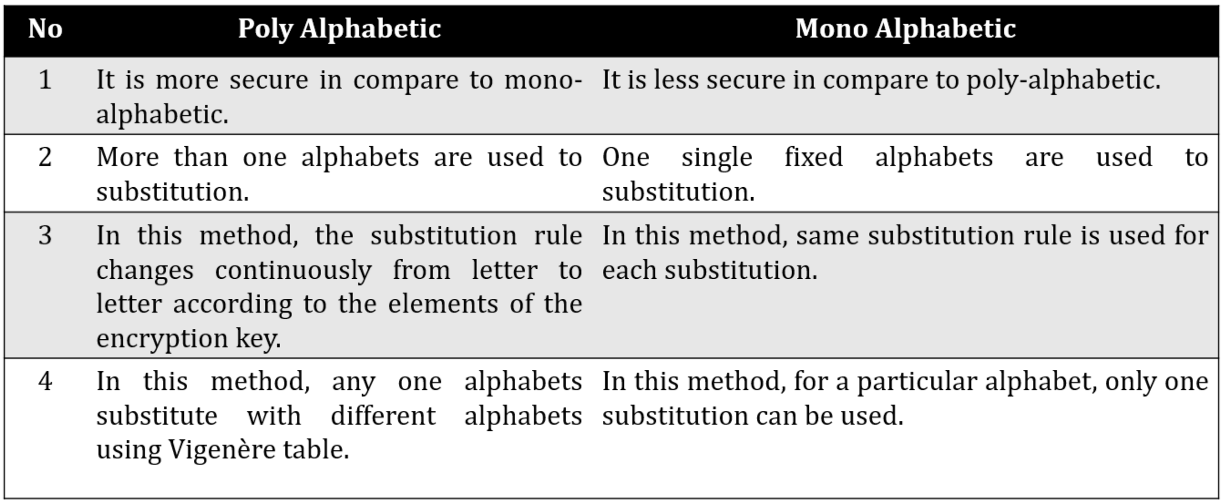
It makes the problem of making large quantities of random keys.

• It also makes the problem of key distribution and protection

10. Define: Replay attack.

A replay attack is one in **which an attacker obtains a copy of an authenticated** packet and later transmits it to the intended destination.

11.What is the difference between a mono alphabetic and a poly alphabetic cipher?



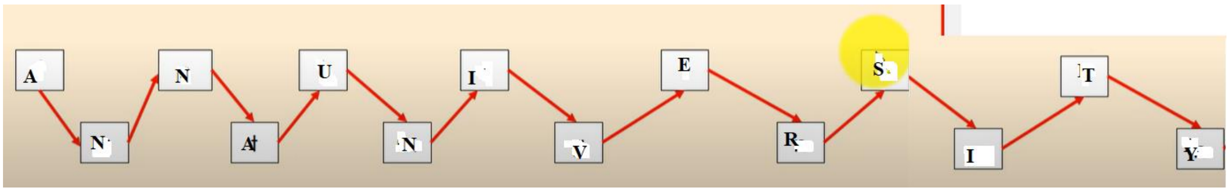
No	Poly Alphabetic	Mono Alphabetic
1	It is more secure in compare to mono-alphabetic.	It is less secure in compare to poly-alphabetic.
2	More than one alphabets are used to substitution.	One single fixed alphabets are used to substitution.
3	In this method, the substitution rule changes continuously from letter to letter according to the elements of the encryption key.	In this method, same substitution rule is used for each substitution.
4	In this method, any one alphabets substitute with different alphabets using Vigenère table.	In this method, for a particular alphabet, only one substitution can be used.

12.Convert the given text "annauniversity" into cipher text using rail fence technique.

<u>Rail Fence Technique</u>

It involves ***<u>writing plain text as a sequence of Diagonals</u>*** and then reading it Row-by-Row to produce cipher text

It is an ***<u>example of transposition</u>***



Cipher text

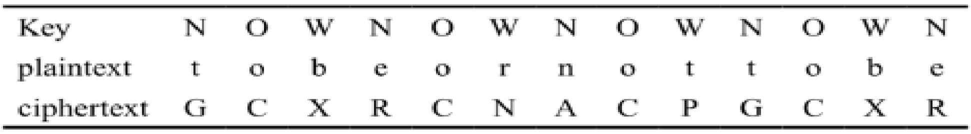
ANUIESTNANVRIY

13,Define steganography

Methods of hiding the existence of a message or other data.This is different than cryptography, which hides the meaning of a message but does not hide the message itself.

14. Encrypt the plaintext tobeornottobe using the vigenere cipher for the key value Now.

n	**O**	**w**	**N**	**o**	**w**	**n**	**o**	**W**	**n**	**o**	**w**	**n**
t	**O**	**b**	**E**	**o**	**r**	**n**	**o**	**T**	**t**	**o**	**b**	**e**
g	**C**	**x**	**R**	**c**	**n**	**a**	**c**	**P**	**g**	**c**	**x**	**r**



Key	N	O	W	N	O	W	N	O	W	N	O	W	N
plaintext	t	o	b	e	o	r	n	o	t	t	o	b	e
ciphertext	G	C	X	R	C	N	A	C	P	G	C	X	R

15. Explain the avalanche effect. [NOV 2007][Nov 2013][MAY 2016]

If there is 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.

16. What are the two approaches to attacking a cipher?[NOV 2007]

The two to attack a cipher are:

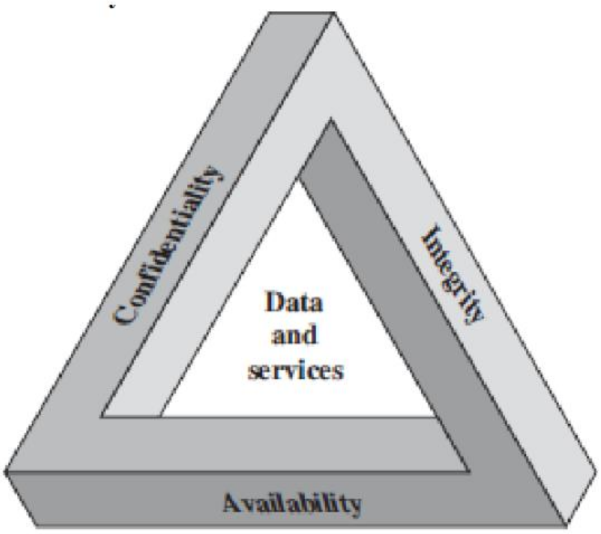
- Cryptanalysis
- Brute-force attack

17.Why is asymmetric cryptography bad for huge data? Specify the reason. (APRIL/MAY 18)

Asymmetric encryption uses **two separate keys** and **more complex *algorithms*** in the encryption and decryption process, which makes it ***slower for encrypting and decrypting large amounts of data.***

18.What are the key principles of security?

Three key objectives of the computer security are **confidentially, integrity and availability**.



1.Confidentiality-Only the intended receiver can understand the information.

Ensures that the information in a computer system and transmitted information are accessible only by authorized parties.

(i)Data confidentiality – assures that private or confidential information is not made available or disclose(make known) to unauthorized individuals.

(ii)Privacy:-

It assures that individuals control what information related to them may be collected and stored.

It also assures that information may be disc by whom and to whom.

2.Integrity [2-marks]

Ensures that only authorized parties are able to modify the stored information and transmitted information.

(i)Data integrity -assures that information and programs are changed only in a specified and authorized manner.

(ii)System integrity:-

Assures that system performs to proposed functions in an undamaged manner. Free from purposed unauthorized manipulate of the system.

3.Availability-assures that system works promptly and service is not denied to authorized Users

19.What are the two basic functions used in the encryption algorithm?

1.Substitution 2.Transposition

1.Substitution

In which each element in the plaintext is mapped into another element.

2.Transposition

In which elements in the plaintext are rearranged .No information is lost.

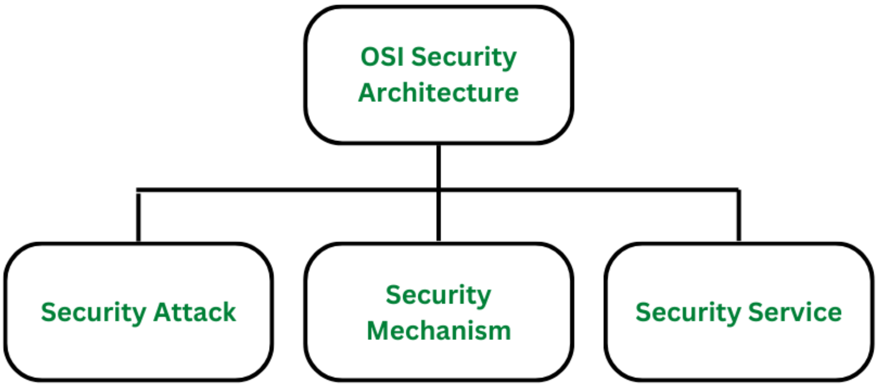
20.List the entities that are to be kept secret in conventional encryption techniques?

Secret Key and encryption algorithm

<u>Part B Questions</u>

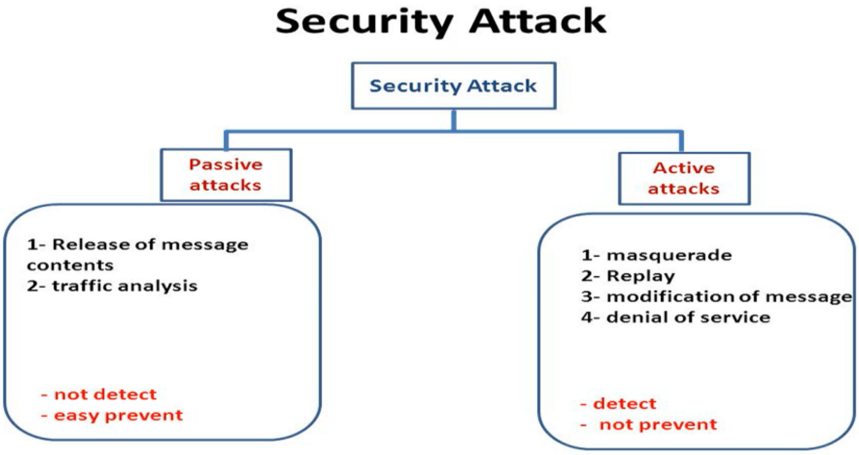
1.(i)Explain OSI Security Architecture model with neat diagram[Nov /Dec 2016]

The **OSI security architecture focuses** on **security attacks, mechanisms, and services**



<u>Definition</u> of ***<u>security attacks, mechanisms, and services</u>***

Threat and Attack –Definition And Difference



(i)Security Attack

Types

1.Passive Attack 2.Active Attack

1.Active Attack

Definition

<u>Types</u>

(i)Masquerade, (ii)Modification of message (iii) Replay (iv) Denial of service.

1.Passive Attack

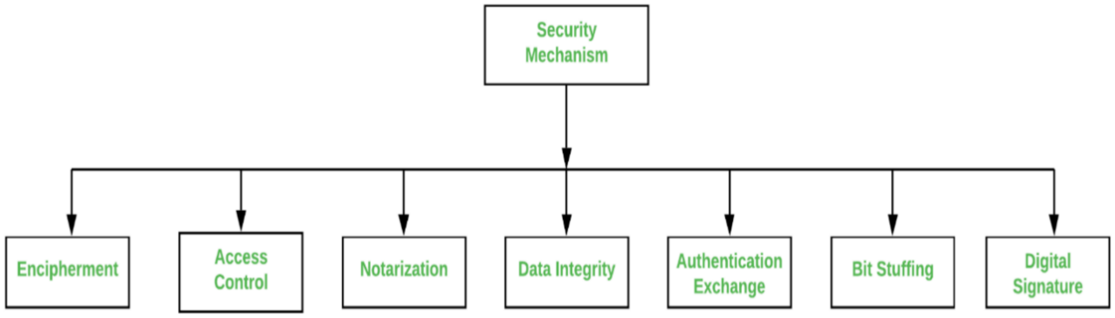
Definition

Types

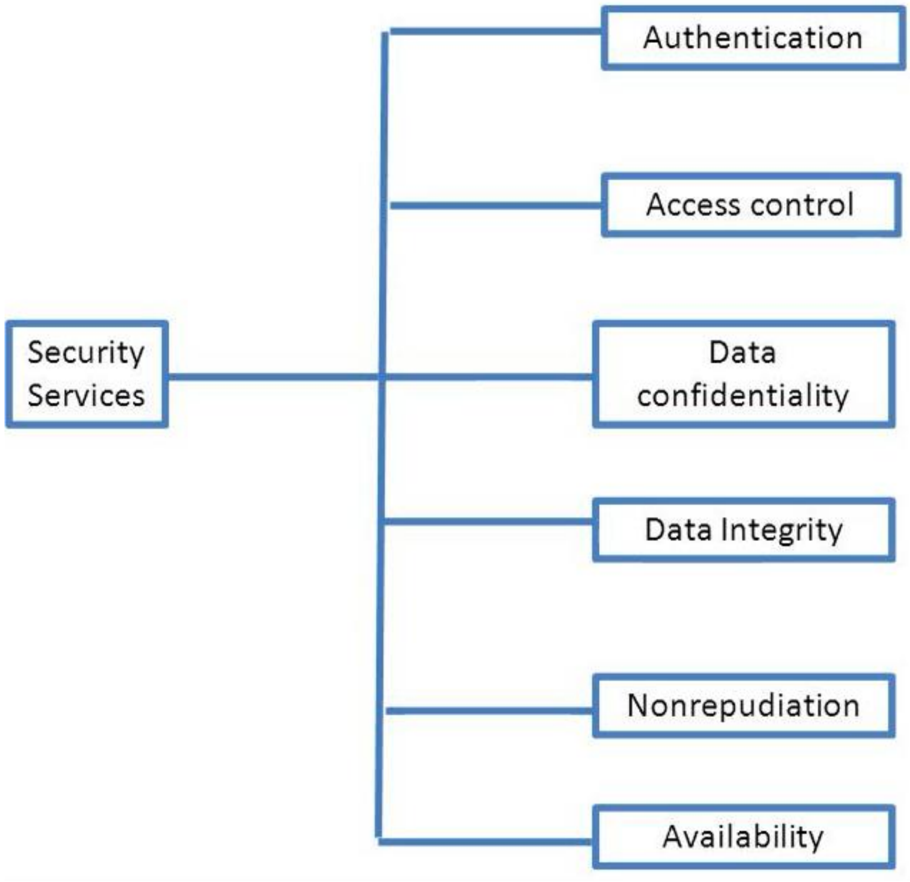
- ❖ Release of message contents
- ❖ Traffic analysis

Difference between Active Attack and passive Attack

(ii)Describe the various security mechanism



Security Services



2.Encrypt the following using play fair cipher using the keyword "MONARCHY."

SWARAJ IS MY BIRTH RIGHT" Use X for blank spaces.(Nov/Dec 17)

3.Describe
(i)Play fair Cipher
(ii)Railfence Cipher
(iii)Vignere Cipher
Answer

(i)Play fair Cipher

- ❖ Definition
- ❖ Algorithm
- ❖ Example
- ❖ Result →Plain Text
    - o Cipher etxt

ii)Railfence Cipher

- ❖ Definition
- ❖ Algorithm
- ❖ Example

iii)Vignere Cipher

- ❖ Definition
- ❖ Algorithm
- ❖ Table
- ❖ Example

4. Explain classical encryption techniques with symmetric cipher and Hill Cipher model?

There are basically two types of symmetric cipher:

Substitution Cipher
Caeser Cipher
Monoalphabetic Cipher
Polyalphabetic Cipher
Playfair Cipher
One Time Pad.
Hill Cipher.
Transposition Cipher

5.(i)**What is steganography?Describe the various techniques used in Steganography?**

- ❖ Definition
- ❖ Example
- ❖ Techniques used
    - o Character Marking
    - o Invisible links
    - o Pin Punctures
    - o Type written correction ribbon
- ❖ Advantages and disadvantages

(ii)What is monoalphabetic cipher?Examine how it differs from Caesar Cipher?

Monoalphabetic cipher is **one where each symbol in plain text is mapped to a fixed symbol in cipher text**.

In Caesar cipher, it can see that it is simply for a hacker to crack the key as Caesar cipher supports only 25 keys in all. This pit is covered by utilizing Monoalphabetic cipher. **In Monoalphabetic**

cipher, the substitute characters symbols supports a random permutation of 26 letters of the alphabet. 26!

Caesar Cipher

- Definiton
- Example

Drawbacks

Easy to break because the key size is fixed.

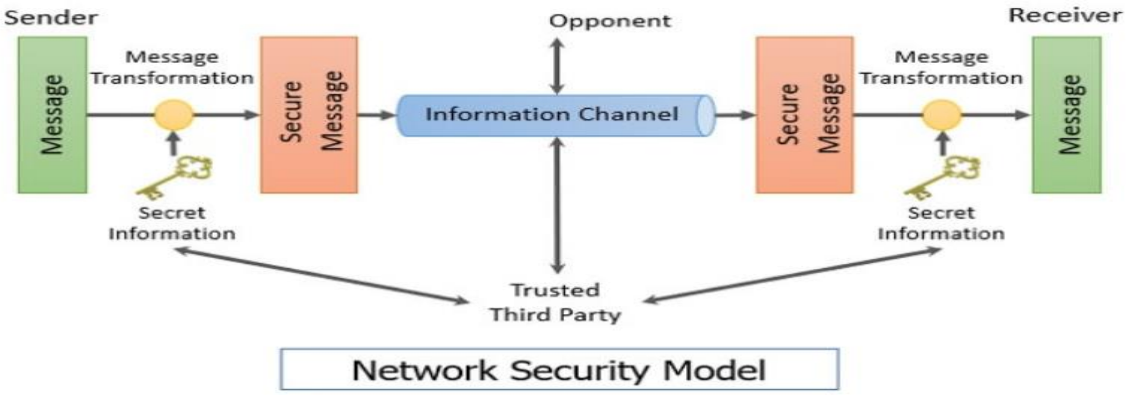
C=(PT+3)MOD 26

MonaAlphabetic Cipher

- Why Mona alphabetic cipher
- Example
- Difference
- Drawbacks

C=(PT+K)MOD 26

6.Explain the network security model and its importance with a neat block diagram?



- Two Components for providing Network Security Model
  - Security related transformation
  - Security information
- Trusted Third party
- Responsibility of trusted third party

- Four basic task to design a particular security service
- Network Access Security Model
- Two types of Threats
- Security Mechanisms
  - Major Procees of Secuirty Mechanisms
    - Gate Keeper
    - Variety of internal Controls.

7.Perform Encyption and decryption using Hill Cipher for the following Messsage :PEN and Key:ACTIVATED

Encryption:

C=KP mod 26

Decryption:

.**Step 1**

$\boxed{P=K^{-1}\ C \bmod 26}$

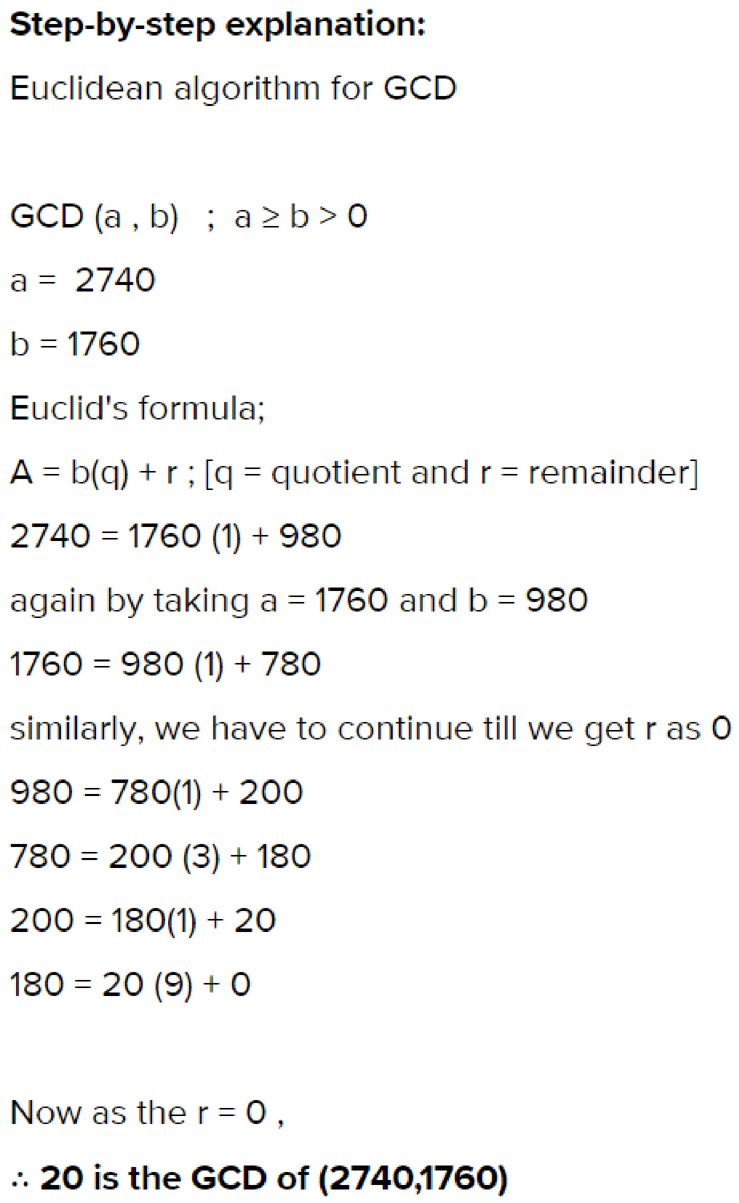
Step 2

$$K^{-1} = \frac{1}{|d|}\ \underline{Adj(K)}$$

CS8792-CRYPTOGRAPHY AND NETWORK SECURITY

UNIT-2: SYMMETRIC CRYPTOGRAPHY

1.Find gcd(2740, 1760) using Euclidean Algorithm(Nov/Dec 2016)



Step-by-step explanation:

Euclidean algorithm for GCD

GCD (a , b) ; $a \geq b > 0$

a = 2740

b = 1760

Euclid's formula;

A = b(q) + r ; [q = quotient and r = remainder]

2740 = 1760 (1) + 980

again by taking a = 1760 and b = 980

1760 = 980 (1) + 780

similarly, we have to continue till we get r as 0

980 = 780(1) + 200

780 = 200 (3) + 180

200 = 180(1) + 20

180 = 20 (9) + 0

Now as the r = 0 ,

∴ 20 is the GCD of (2740,1760)

2.Find gcd(1970,1000) using Euclidean Algorithm

To find the greatest common divisor (GCD) of 1970 and 1000 using the Euclidean algorithm with the formula GCD(a, b) = GCD(b, a mod b), you can follow these steps:

GCD(1970, 1000) = GCD(1000, 1970 % 1000)
GCD(1000, 970) = GCD(970, 1000 % 970)
GCD(970, 30) = GCD(30, 970 % 30)
GCD(30, 10) = GCD(10, 30 % 10)
GCD(10, 0)

Since the remainder has become 0, we can stop. The GCD of 1970 and 1000 is 10, which is the last non-zero remainder in the Euclidean algorithm process.

So, GCD(1970, 1000) = 10.

3.Determine the gcd(24140,16762)using Euclid's Algorithm

The **formula GCD(a, b) = GCD(b, a mod b),** you can follow these steps:

GCD(24140, 16762) = GCD(16762, 24140 % 16762)
GCD(16762, 7378) = GCD(7378, 16762 % 7378)
GCD(7378, 2006) = GCD(2006, 7378 % 2006)
GCD(2006, 363) = GCD(363, 2006 % 363)
GCD(363, 170) = GCD(170, 363 % 170)
GCD(170, 23) = GCD(23, 170 % 23)
GCD(23, 3) = GCD(3, 23 % 3)
GCD(3, 2) = GCD(2, 3 % 2)
GCD(2, 1) = GCD(1, 2 % 1)

GCD=2

4.Find gcd(21,300) using Euclid's Algorithm

To find the greatest common divisor (GCD) of 21 and 300 using the Euclidean algorithm with the formula GCD(a, b) = GCD(b, a mod b), you can follow these steps:

GCD(21, 300) = GCD(300, 21 mod 300)
GCD(300, 21) = GCD(21, 300 mod 21)
GCD(21, 15) = GCD(15, 21 mod15)
GCD(15, 6) = GCD(6, 15 mod6)
GCD(6, 3) = GCD(3, 6 mod 3)
GCD(3, 0)

At this point, the remainder becomes 0, so we can stop. The last non-zero remainder is 3.

So, GCD(21, 300) = 3.

5.Find gcd(45,6)using Euclidean algorithm.

To find the greatest common divisor (GCD) of 45 and 6 using the Euclidean algorithm with the following formula:

GCD(a, b) = GCD(b, amod b)

Let's apply this formula step by step:

GCD(45, 6) = GCD(6, 45 % 6)
GCD(6, 3) = GCD(3, 6 % 3)
GCD(3, 0)

Since the second number becomes 0, we have our result:

GCD(45, 6) = 3

So, the **GCD of 45 and 6 is 3.**

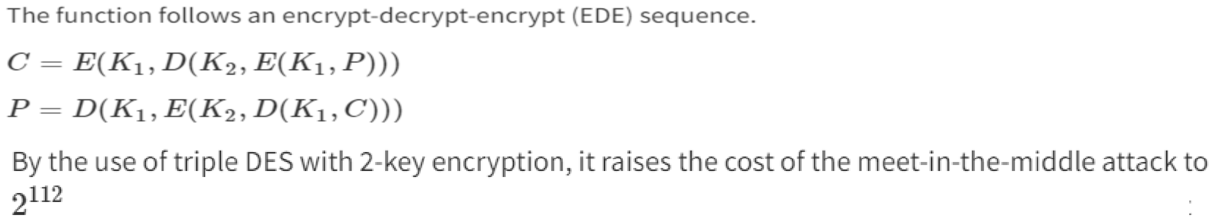
6.Brief the strength of Triple DES

Triple DES with 2 Keys

❖ It uses ***three stages of DES*** for ***encryption and decryption***.

❖ The 1st, 3rd stage use ***K1 key and 2nd stage use K2 key***.

- To make ***triple DES compatible with single DES***, the middle stage uses decryption in the encryption side and encryption in the decryption side.
- It's much stronger than double DES.
- The function follows an encrypt-decrypt-encrypt (EDE) sequence



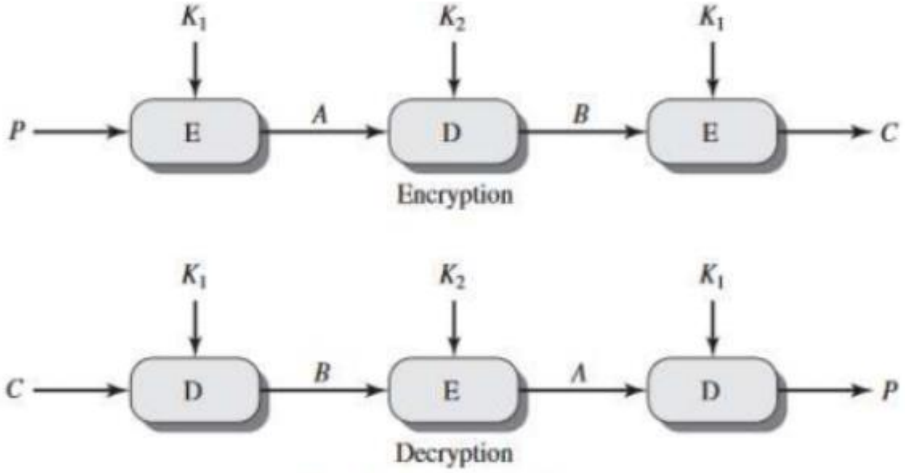
The function follows an encrypt-decrypt-encrypt (EDE) sequence.

$C = E(K_1, D(K_2, E(K_1, P)))$

$P = D(K_1, E(K_2, D(K_1, C)))$

By the use of triple DES with 2-key encryption, it raises the cost of the meet-in-the-middle attack to 2^{112}

It has the drawback of requiring a key length of $56 \times 3 = 168$ bits which may be somewhat



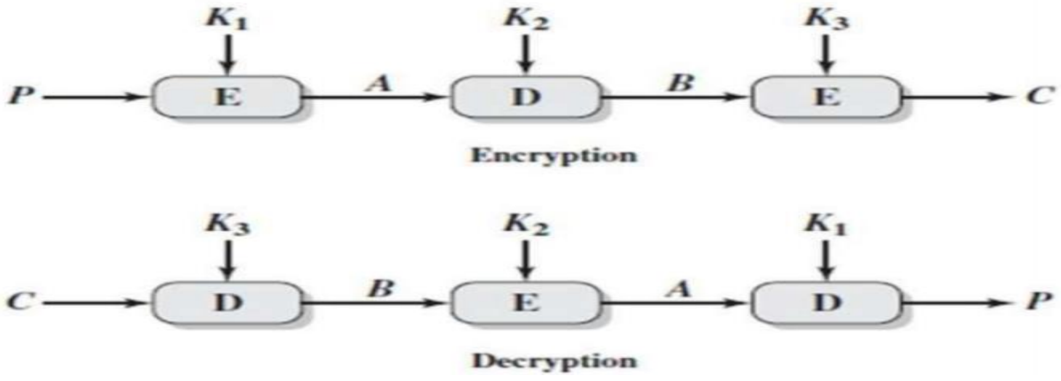
(b) Triple encryption

Triple DES with 3-key

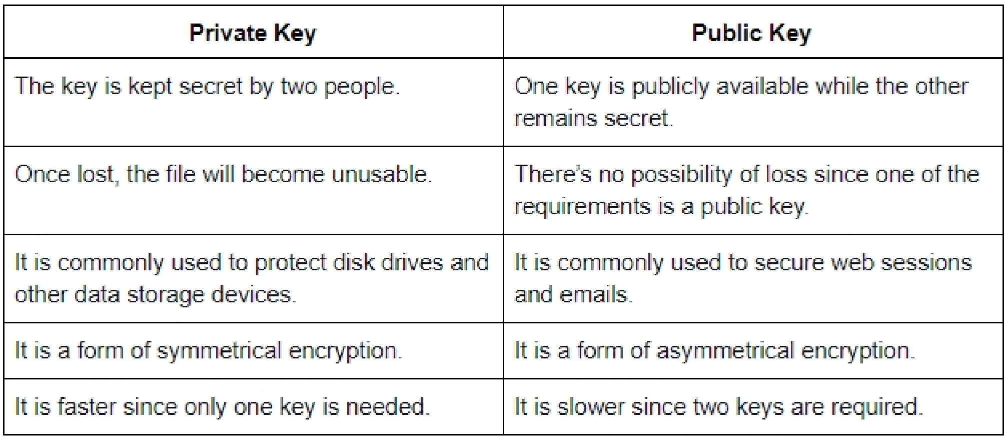
Although the attacks just described appear impractical, anyone using two key 3DES
It uses three stages of DES for encryption and decryption. The 1st, use K1key and 2nd stage use K2 key and 3rd stage k3 key

Three-key 3DES has ***an effective key length of 168 bits*** and is defined as

$$C = \mathrm{E}(K_3, \mathrm{D}(K_2, \mathrm{E}(K_1, P)))$$

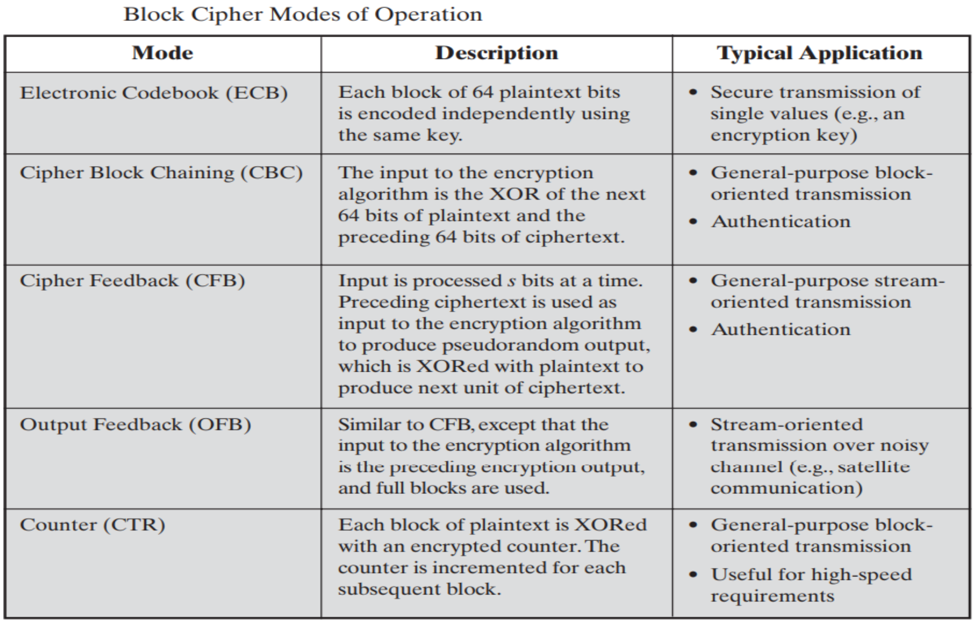


7.State the difference between private key and public key Algorithm



Private Key	Public Key
The key is kept secret by two people.	One key is publicly available while the other remains secret.
Once lost, the file will become unusable.	There's no possibility of loss since one of the requirements is a public key.
It is commonly used to protect disk drives and other data storage devices.	It is commonly used to secure web sessions and emails.
It is a form of symmetrical encryption.	It is a form of asymmetrical encryption.
It is faster since only one key is needed.	It is slower since two keys are required.

8.Give the five modes of operation of block cipher

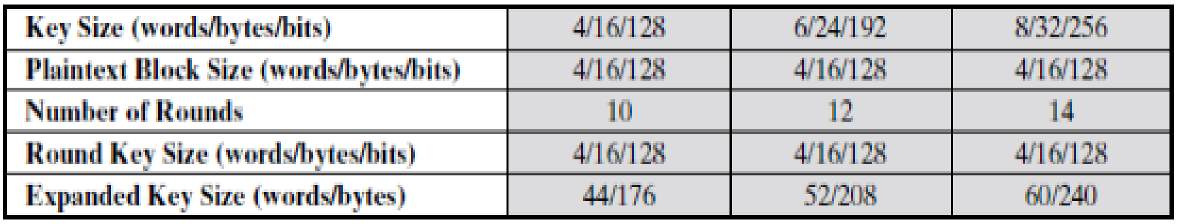


Block Cipher Modes of Operation

Mode	Description	Typical Application
Electronic Codebook (ECB)	Each block of 64 plaintext bits is encoded independently using the same key.	• Secure transmission of single values (e.g., an encryption key)
Cipher Block Chaining (CBC)	The input to the encryption algorithm is the XOR of the next 64 bits of plaintext and the preceding 64 bits of ciphertext.	• General-purpose block-oriented transmission • Authentication
Cipher Feedback (CFB)	Input is processed *s* bits at a time. Preceding ciphertext is used as input to the encryption algorithm to produce pseudorandom output, which is XORed with plaintext to produce next unit of ciphertext.	• General-purpose stream-oriented transmission • Authentication
Output Feedback (OFB)	Similar to CFB, except that the input to the encryption algorithm is the preceding encryption output, and full blocks are used.	• Stream-oriented transmission over noisy channel (e.g., satellite communication)
Counter (CTR)	Each block of plaintext is XORed with an encrypted counter. The counter is incremented for each subsequent block.	• General-purpose block-oriented transmission • Useful for high-speed requirements

9.List the parameters (block size,key size and no of rounds) for the three AES versions.

- ❖ The algorithm is referred to as **AES-128, AES-192, orAES-256,** depending on the **key length.**



Key Size (words/bytes/bits)	4/16/128	6/24/192	8/32/256
Plaintext Block Size (words/bytes/bits)	4/16/128	4/16/128	4/16/128
Number of Rounds	10	12	14
Round Key Size (words/bytes/bits)	4/16/128	4/16/128	4/16/128
Expanded Key Size (words/bytes)	44/176	52/208	60/240

10.What are the primitive operations used in RC4?

The primitive operation used in RC4 is bit wise Exclusive-OR (XOR) operation.

11. Compare DES and AES

AES	DES
AES stands for ***Advanced Encryption Standard***	DES stands for ***Data Encryption Standard***.
AES allows the data length (plain text size) of 128, 192, and 256 bits.	Data encryption standard takes 64-bit plaintext as input and creates 64-bit Ciphertext i.e. it encrypts data in a block of size 64-bits per block.
AES divide plaintext into 16 bytes (128-bit) blocks and treats each block as a 4×4 State array and supporting three different key lengths, 128, 192. and 256 bits.	In DES plaintext message is divided into size 64-bit block each and encrypted using the 56-bit key at the initial level.
The number of rounds is 10, which is for the case when the encryption key is 128 bits long. (As mentioned earlier, the number of rounds is 12 when the key is 192 bits and 14 when the key is 256.)	The left plaintext and right plaintext goes through 16 rounds of encryption process along with 16 different keys for each round.
AES was designed by Vincent Rijmen and Joan Daemen.	DES was designed by IBM.
AES is faster.	DES is comparatively slower.
AES has a large secret key comparatively hence, more secure.	DES has a smaller key which is less secure.
Sub bytes, Shif trows, Mix columns, Add round keys.	Expansion Permutation, Xor, S-box, P-box, Xor, and Swap.
10 rounds for 128-bit algo 12 rounds for 192-bit algo 14 rounds for 256-bit algo	16 rounds

12.Define field and Ring in Number Theory?

A **ring** R, sometimes denoted by {R, +, x}, is a set of elements with two binary operations, called addition and multiplication,[2] such that for all a, b, c in R the following axioms are obeyed: Generally, we do not use the multiplication symbol, x, but denote multiplication by the concatenation of two elements.

A **field** F, sometimes denoted by {F, +, x}, is a set of elements with two binary operations, called addition and multiplication, such that for all a, b, c in F

13.List the entities that are to be kept secret in conventional encryption techniques

Two main requirements are needed **for secure use of conventional encryption**:

(i). A **strong encryption algorithm** is needed. It is desirable that the algorithm should be in such a way that, even the attacker who knows the algorithm and has access to one or more cipher texts would be unable to decipher the ciphertext or figure out the key.

(ii).The **secret key** must be distributed among the sender and receiver in a very secured way. If in any way the key is discovered and with the knowledge of algorithm, all communication using this key is readable.

The important point is that the ***security of conventional encryption*** depends on the **secrecy of the key**, not ***the secrecy of the algorithm*** i.e. it is not necessary to keep the algorithm secret, but only ***the key is to be kept secret***

14.What is the residues of 6 when n=8

When the integer a is divided by the integer n, **the remainder r** is referred to as the **residue**.

Equivalently,$\boxed{\mathbf{r=a\ \ mod\ n}}$.

6 divided by 8 equals 0 with a remainder of 6.

So, the residue of 6 when n = 8 is 6.

15. Write down the purpose of the S-Boxes in DES?

S-boxes are ***non-linear transformations*** of a few input bits that **provide confusion.**

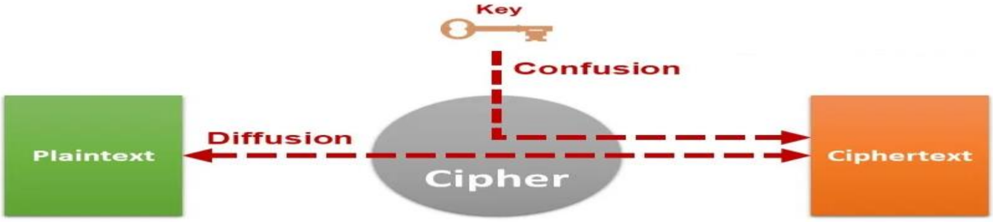
16. Define : Diffusion.

Diffusion

- If any of the ***characters in the plaintext is changed***,then simultaneously ***several characters of the ciphertext should also be changed.***
- It is a **classical transposition cipher**.
- Note:**Diffusion** hides the relation between the **ciphertext and plaintext**.
- **P-box or transposition cipher**

Confusion

- In Confusion **each character of ciphertext** depends on a **different part of a key**.
- In confusion **the key does not directly** related to **ciphertext.**
- It is a classical **substitution cipher.**
- Note:**Confusion** hides the relation between the **ciphertext and key**.
- **S-box or Substitution cipher**



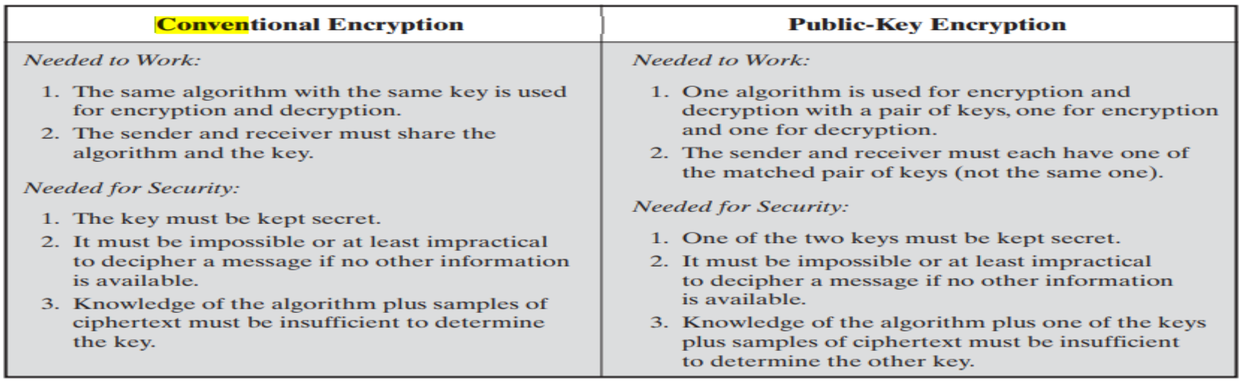
17. Define : Primality test. ?

A **primality test** is an algorithm **for determining whether an input number is prime**.

18. Why modular arithmetic has been used in cryptography?

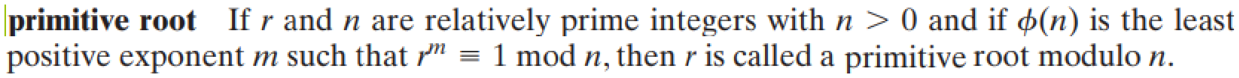
Modular arithmetic allows us to easily create groups, rings and fields which are fundamental building blocks of most modern public-key cryptosystems.

19. State the difference between conventional encryption 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.Define primitive root



primitive root If r and n are relatively prime integers with $n > 0$ and if $\phi(n)$ is the least positive exponent m such that $r^m \equiv 1 \bmod n$, then r is called a primitive root modulo n.

21. What are the disadvantages of double DES?

The disadvantages of double DES is Meet in the middle Attack

Double DES results in a ***mapping that is not equivalent to a single DES*** encryption.

But there is a way ***to attack this scheme***, one that does not depend on any particular property of DES but that will work against any block encryption cipher. The algorithm, known as a **meet-in-the-middle attack**

22.What is the Meet in the Middle Attack?

Definition

- ❖ This attack involves **encryption from one end and decryption from other end** and then matching the results in the middle is called as ***Meet in the Middle attack***
- ❖ This attack requires knowing **some plain text and cipher text pairs**

23. List AES Evaluation criteria?

Three categories of criteria were as follows

(i)Security (ii)Cost (iii)Algorithm and Implementation characteristics

24.List important design considerations for a stream cipher.

- ❖ The **encryption sequence** should have a **large period**.
- ❖ The **key stream** should approximate the **properties of a true random number stream as close as** possible.
- ❖ The output of the **pseudorandom number generator** is conditioned on the value of the input key.

Part B Questions

1.Draw the functionality diagram (functionality in one round) of DES with number of bits in each flow of data.

[or]

Describe DES algorithm with neat diagram and explain the steps.

Answer

DES Definition

Steps

(i)Initial permutation

(ii)16 fiestal rounds

(iii)Swapping /left-right swap

(iv) Final Permutation /Inverse Initial Permutation

Steps in Function Block

1. Expansion Permutation
2. Definition of S-Boxes
3. Permutation Function
4. Inverse Permutation

2. Explain with sample data: Four transformations in AES.

Or

What do you mean by AES Diagrammatically illustrate the structure of AES and describe the steps in AES encryption process with example.

The **first N - 1 round** consist of **four distinct transformation functions:**

(i)Sub Bytes,

(ii)Shift Rows,

(iii)Mix Columns, and

(iv) AddRoundKey.

3. Discuss the properties that are to be satisfied by Groups, Rings and Fields.

Group, Ring and Fields Definition

Group, Ring and Fields Properties

4. Explain the Key Generation, Encryption and Decryption of SDES algorithm in detail

SIMPLIFIED DATA ENCRYPTION STANDARD (S-DES)

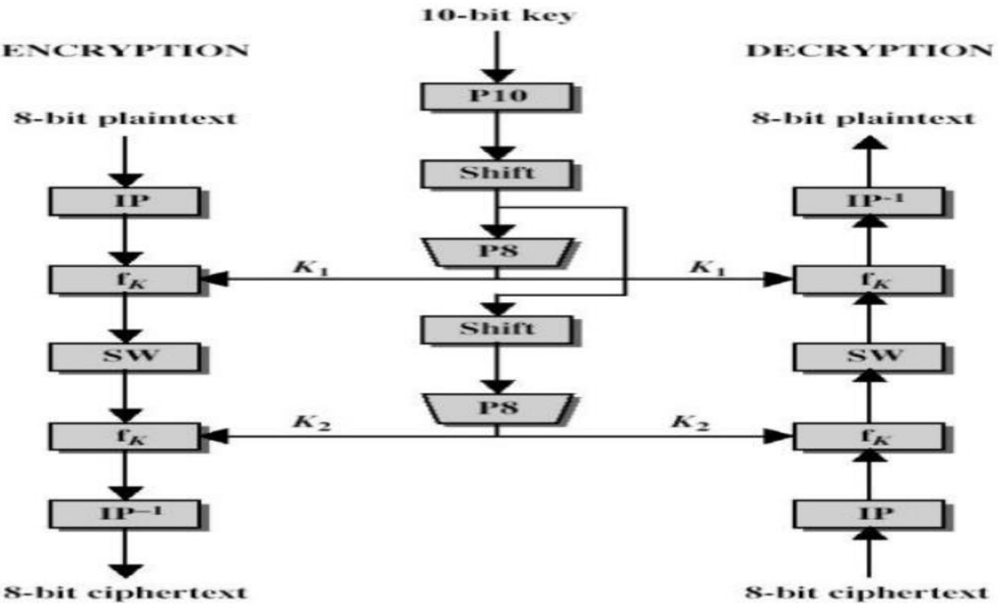


Figure 2.5 Overview of S-DES Algorithm

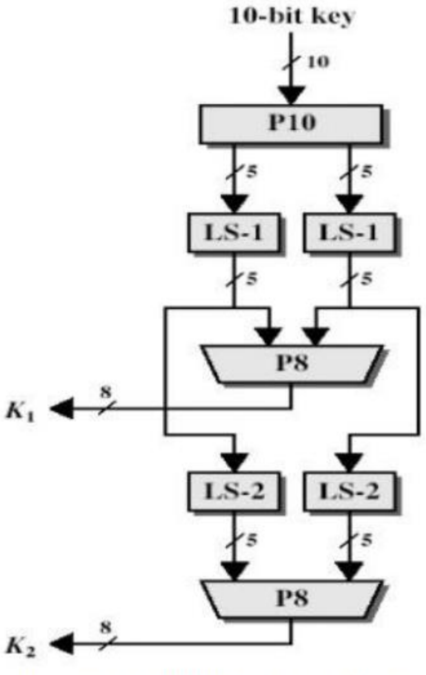


Figure 2.6 S-DES Key Generation

5. Block Cipher Modes of Operation

(i)**Electronic Code Book**

(ii) Cipher Block Chaining Mode

(ii) Cipher Feedback Mode

(ii) Output Feedback Mode

- Definition
- Block diagram
- Advantages and Disadvantages

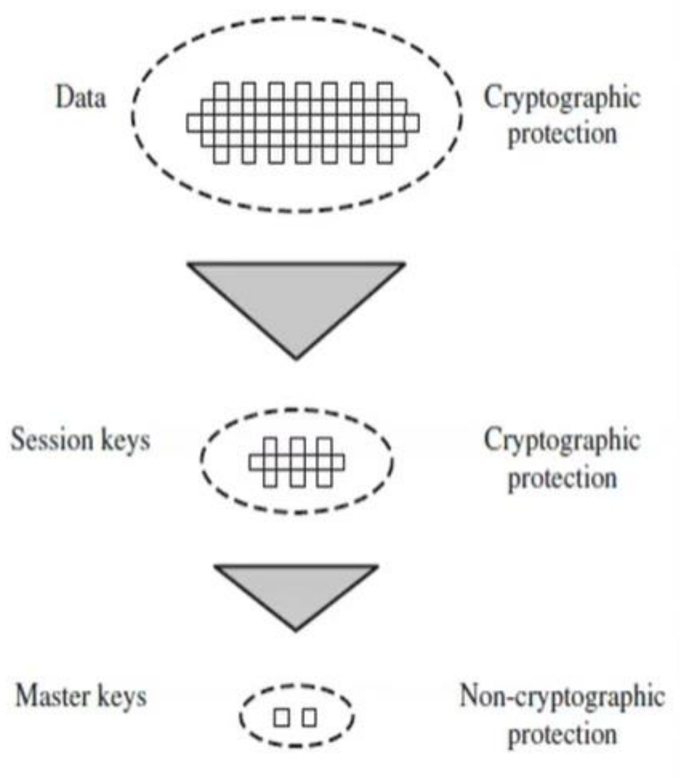
6. Design Principles of block cipher

- DES Design Criteria
  - Criteria for the S-boxes
  - Criteria for the permutation P
  - Number of Rounds
- Design of Function F
- Key Schedule Algorithm

7. Key Distribution in Symmetric Encryption

Key Distribution between two parties

Symmetric Key Distribution using Symmetric Encryption



- Key Distribution Scenario
- A transparent key control scheme

UNIT III PUBLIC KEY CRYPTOGRAPHY

1. Write the difference between public key and private key crypto systems? (APR/MAY 2012&APR/MAY2017)(Analysis)

Private Key encryption uses a single key to both encrypt and decrypt messages. It must be present at both the source and destination of transmission to allow the message to be transmitted securely and recovered upon receipt at the correct destination. Public key systems use a pair of keys, each of which can decrypt the messages encrypted by the other. Provided one of these keys is kept secret (the private key), any communication encrypted using the corresponding public key can be considered secure as the only person able to decrypt it holds the corresponding private key.

2. State whether symmetric and asymmetric cryptographic algorithms need key exchange? (APR/MAY2014)(Analysis)

Key exchange is a method in cryptography by which cryptographic keys are exchanged between two parties, allowing use of a cryptographic algorithm. Symmetric encryption requires the sender and receiver to share a secret key. Asymmetric encryption requires the sender and receiver to share a public key. If the cipher is a symmetric key cipher, both will need a copy of the same key. If an asymmetric key cipher with the public/private key property, both will need the other's public key.

3. List the Authentication requirements? (APR/MAY 2014) (NOV/DEC2016)

The authentication is provided for the following attacks

- Disclosure
- Traffic analysis
- Masquerade
- Content modification
- Sequence modification
- Timing Modification
- Source repudiation
- Destination Repudiation

4.Point out the types of cryptanalytic attacks?(NOV/DEC 2014)

The two types of cryptanalytic attacks includes the

- Attacks on hash functions
- Attacks on message authentication codes

5. What is Man in the Middle attack?

This is the cryptanalytic attack that attempts to find the value in each of the range and domain of the Composition of two functions such that the forward mapping of one through the first function is the same as the inverse image of the other through the second function-quite literally meeting in the middle of the Composed function.

6. What is the Fermat’s theorem? (Nov/Dec 2017)? (NOV/DEC 2022)

Fermat‟s theorem states the following: If p is prime and a is a positive integer not divisible by p, then

7. What is the use of Fermat’s theorem?(NOV/DEC 2021)

- This theorem is central to the calculus method of determining maxima and minima: in one dimension, one can find extreme by simply computing the stationary points (by computing the zeros of the derivative), the non- differentiable points, and the boundary points, and then investigating this set to determine the extreme.
- One can do this either by evaluating the function at each point and taking the maximum, orby analyzing the derivatives further, using the first derivative test, the second

Derivative test, or the higher-order derivative test.
□ in dimension above 1, one cannot use the first derivative test any longer, but the second
Derivative test and higher-order derivative test generalize.

8. Describe Chinese remainder theorem.

The Chinese remainder theorem is a result about congruences in number theory and its generalizations in abstract algebra. In its basic form, the Chinese remainder theorem will determine a number n that when divided by some given divisors leave given remainders.

9. Define Euler's theorem and it's application? (APRIL/MAY 18)

Euler's theorem states that for every a and n that is relatively prime:

a

$\Phi(n) \equiv 1 \bmod n$

10.Define Euler's totient function or phi function and their applications?

The Eulers totient function states that, it should be clear for a prime number p,

$\Phi(p) = p-1$

11. Describe in general terms an efficient procedure for picking a prime number?

The procedure for picking a prime number is as follows:

1. Pick an odd integer n at random (eg., using a pseudorandom number generator).
2. Pick an integer a<n at random.
3. Perform the probabilistic primality test, such as Miller-Rabin. If n fails the test, reject the value n and go to step1.
4. If n has passed a sufficient number of tests, accept n; otherwise, go to step2.

12. Define Fermat Theorem? (Apr/May 17)

Fermat Theorem states the following: If p is prime and a is a positive integer not divisible by p, then Ap-1≡ 1 mod p

13. What is discrete Logarithm?

Discrete logarithms are fundamental to a number of public-key algorithms, including Diffie Hellman key exchange and the digital signature algorithm. Consider the equation Given g, x, and p, it is a straightforward matter to calculate y. At the worst, we must perform x repeated multiplications, and algorithms exist for achieving greater Efficiency.

14. User A and B exchange the key using Diffie-Hellman algorithm. Assume □ = 5 q=11
XA =2 XB =3. Find the value of YA , YB andk?(Analysis)

YA =□

X

A modq = 25mod 11 =3

YB = □

XKB modq = 125mod 11 =4

= (YA)

XKB modq = 27mod 11 =5

= (YB)

X

A modq = 16mod 11 =5

15. Perform encryption and decryption using RSA Alg. for the following. (NOV/DEC 2017)
P=7; q=11;e=17;M=8. (APRIL/MAY18)

Soln:
n = pq
n = 7*11=77
Φ(n) =(p-1)(q-1)
=6*10 =60
e =17 , d =27
C = M e mod n
C = 817 mod 77
= 57
M = Cd mod n
= 5727 mod 77
= 8

16. Mention any three Primality Testing Methods.

1. Naïve Algorithm
2. Fermat’s Primality Test
3. Miller-Rabin Primality Test

17. Write the formula for Encryption and Decryption in RSA (NOV/DEC 2021).

For Decryption C = Me mod n
For Encryption M = Cd mod n

18. Consider the RSA encryption method with p=11 and q=17 as the two primes.Find n and □(n). (Evaluate) [NOV/DEC19](NOV/DEC 2020)

n = p x q = 17 x 11 = 187
□(n) = (p-1)(q-1) = (17-1)(11-1)
= 16 (10)
= 160.

19.What are the functions used to produce an authenticator? (NOV/DEC 2022)

Conventional encryption can serve as Authenticator. Conventional encryption provides authentication aswell as confidentiality .Requires recognizable plaintext or other structure to distinguish between well- formed legitimate plaintext and meaningless random bits.

20.State whether symmetric and asymmetric cryptographic algorithms need key exchange? (APR/MAY 2014)(Analysis)

- Key exchange is a method in cryptography by which cryptographic keys are exchanged between two parties, allowing use of a cryptographic algorithm.
- Symmetric encryption requires the sender and receiver to share a secret key.
- Asymmetric encryption requires the sender and receiver to share a public key.
- If the cipher is a symmetric key cipher, both will need a copy of the same key.
- If an asymmetric key cipher with the public/private key property, both will need the other's public key

21.What is the Fermat’s theorem? (Nov/Dec 2017)? (Remember)

Fermat’s theorem states the following: If *p* is prime and *a* is a positive integer not divisible by *p*, then

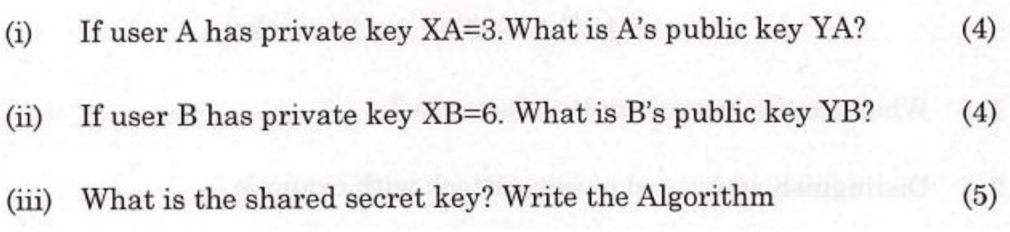
$$a^{p-1} \equiv 1 (\bmod p)$$

Uses of Fermat’s Theorem

- This theorem is method of ***determining maxima and minima***: in one dimension, one can find ***extreme by simply computing the stationary points*** (by computing the zeros of the derivative), the non-differentiable points, and the boundary points, and then investigating this set to determine the extreme. One can do this either ***by evaluating the function at each point and taking the maximum, or by analyzing the derivatives*** further, using the first derivative test, the second derivative test, or the higher-order derivative test.
- In dimension above 1, one cannot use the first derivative test any longer, but the second derivative test and higher-order derivative test generalize.

Part B Questions

1. User A and B use the Diffie Hellman key exchange technique,a common prime q=11 and a primitive root alpha =7



(i) If user A has private key XA=3.What is A's public key YA? (4)

(ii) If user B has private key XB=6. What is B's public key YB? (4)

(iii) What is the shared secret key? Write the Algorithm (5)

Answer:

- Define Diffie-Hellman Algorithm
- Diffie-Hellman formula:

Y_A = (alpha^X_A) mod q
Y_B = (alpha^X_B) mod q
K= Y_B^X_A mod q
K= Y_A^X_B mod q

2. Identify the possible threats for RSA algorithm and list their counter measures.
Perform Encryption and decryption using RSA algorithm with p=3 q=11 e=7 and N=5

- **Define RSA Algorithm**
- **List the possible threats**
- **Denote formulas**
- **Solve the problem**

3. Demonstrate the DH key exchange methodology using following key values: p=11 ,g=2 X_A =9 , 4 X_B =4 .

Answer

- Define Diffie-Hellman Algorithm
- Diffie-Hellman formula:

Y_A = (alpha^X_A) mod q
Y_B = (alpha^X_B) mod q
K= Y_B^X_A mod q
K= Y_A^X_B mod q

- Calculate necessary values

4.State Chinese Remainder theorem and find X for the given set of congruent equations using CRT. X=2(mod 3) , X=3(mod 5) , X = 2(mod 7).[NOV 2016]

Or

State Chinese Remainder Theorem and find X for the given set of congruent equations using CRT

X=1(mod 5)
X=2(mod 7)
X=3(mod 9)
X=4(mod 11) (13 Marks Nov/Dec 2020]

Answer:

5(i).Find the gcd (6432,768)by using Extended Euclidean algorithm

(ii)Find φ(519)

- **Define Euclidean algorithm**
- **List the steps**
- **Solve the problem using the above steps**

6.State Chinese Remainder Theorem and find X for the given set of congruent equations using CRT

X=10(mod 2)
X=7(mod 9)
X=3(mod 5) (13 Marks Apr/May 2023]

(ii)Find 103^{27} mod 467

- Definition
- Algorithm
- Problem with formulas

State and prove Fermat's theorem.

- Definition
- Proof
- Example problem

3.Explain RSA algorithm,perform encryption and decryption to the system with p=7 and q=11 e=17 and M=8

- Definition
- Algorithm
- Problem

7.Users alice and bob use the diffie hellman key exchange technique with a common prime q=83 and a primitive root α=5.

i) if Alice has a private key XA=6, what is Alice's public key YA? (6 marks)
ii) if bob has a private key XB =10 what is bob's public key YB? (6 marks)
iii) What will be shared secret key (8 marks)

- Define Diffie-Hellman Algorithm
- Diffie-Hellman formula:

  Y_A = (alpha^X_A) mod q
  Y_B = (alpha^X_B) mod q
  K= Y_B^X_A mod q
  K= Y_A^X_B mod q
- Calculate necessary values

8.Explain Diffie-Hellman Key exchange algorithm in detail(Apr/May 2017)
Or
Explain briefly about Diffie-Hellman Key exchange algorithm with its merits and demerits [Apr/May 2019]

- Definiton
- Algorithm
- Example Problem
- Merits and Demerits

9.With a neat sketch explain the Elliptic curve cryptography with an example[Apr/May 2018]

- Definition
- Mathematical Equation
- ECC Diffie Hellman KeyExchange
- Explanation
- Decryption
- Computational effort for CryptAnalysis

11.Find the secret key shared between user A and user B usingDiffie Hellman algorithm for the following q=353,α(primitive root)=3 ,X_A=45 and X_B=50

- Definition
- Formula
- Given Values
- To be find
- Refer Classwork Note Book

12.Describe RSA algorithm

Definiton
Algorithm
Explanation
Example Problem

13. Perform encryption and decryption using RSA algorithm for the following with p=7 and q=11 e=7 M-9.[Apr/May 2018]

- ❖ Definiton
- ❖ Algorithm
- ❖ Problem with both encryption and decryption

14.Explain Public Key Cryptography and when it is preferred?[Nov/Dec 2019]

- ❖ Definition
- ❖ Diagram Publickey cryptography
- ❖ Characteristics of Public key cryptosystems
- ❖ Components of PublicKey Cryptography

UNIT IV – MESSAGE AUTHENTICATION AND INTEGRITY

PART – A

1.Name the four requirements defined by Kerberos[Nov/Dec 2022]

Requirements for Kerberos

Secure

An **opponent does not find** it to be the weak link.

Reliable

The system should be able to back up another.

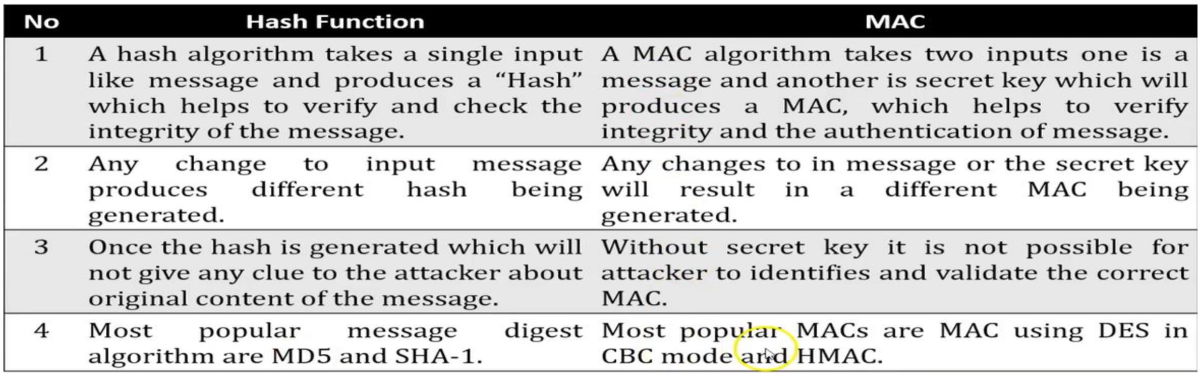
Transparent

An user should not be aware of authentication

Scalable

The system supports large number of clients and servers

2. Difference between MAC and Hash Function?[Nov/Dec2022]



No	Hash Function	MAC
1	A hash algorithm takes a single input like message and produces a "Hash" which helps to verify and check the integrity of the message.	A MAC algorithm takes two inputs one is a message and another is secret key which will produces a MAC, which helps to verify integrity and the authentication of message.
2	Any change to input message produces different hash being generated.	Any changes to in message or the secret key will result in a different MAC being generated.
3	Once the hash is generated which will not give any clue to the attacker about original content of the message.	Without secret key it is not possible for attacker to identifies and validate the correct MAC.
4	Most popular message digest algorithm are MD5 and SHA-1.	Most popular MACs are MAC using DES in CBC mode and HMAC.

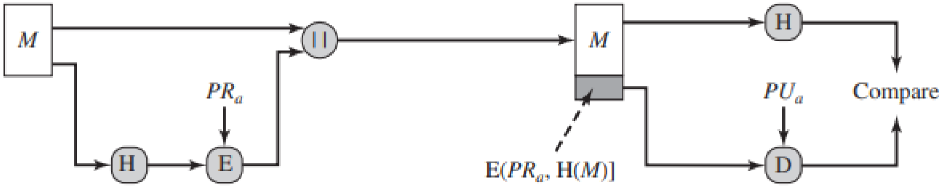
3. What is meant by padding? And, why padding is required?[Nov/Dec 2021]

- ❖ Padding in cryptography refers to **the process of adding extra bits or bytes** to data before it is encrypted or processed by a cryptographic algorithm.
- ❖ Padding is an essential aspect of many **cryptographic processes, ensuring that data** is processed and encrypted in a secure and consistent manner.

In SSL, the padding added prior to encryption of user data is the minimum amount required so that the total size of the data to be encrypted is a multiple of the cipher's block length.

In TLS, the padding can be any amount that results in a total that is a multiple of the cipher's block length, up to a maximum of 255 bytes.

4. Draw functional diagram of RSA based Digital Signature.[Nov/Dec 2021]



(a) RSA approach

5.How is the security of a MAC function expressed ? (NOV/DEC 2017)

The security of a MAC function expressed in terms of the probability of successful forgery with a given amount of time spent by the forger and a given number of message-MAC pairs created with the same key.

6.Mention the significance of signature function in Digital Signature Standard (DSS) approach. (NOV/DEC 2017)

A digital signature is represented in a computer as a string of binary digits. A digital signature is computed using a set of rules and a set of parameters such that the identity of the signatory and integrity of the data can be verified. An algorithm provides the capability to generate and verify signatures. Signature generation makes use of a private key to generate a digital signature. Signature verification makes use of a public key which corresponds to, but is not the same as, the private key.

7.Write a simple authentication dialogue used in Kerberos. (NOV/DEC 2017)

$$\textbf{(1)}\ \ \mathrm{C} \rightarrow \mathrm{AS}: \quad ID_C \| P_C \| ID_V$$

$$\textbf{(2)}\ \ \mathrm{AS} \rightarrow \mathrm{C}: \quad Ticket$$

$$\textbf{(3)}\ \ \mathrm{C} \rightarrow \mathrm{V}: \quad ID_C \| Ticket$$

$$Ticket = E(K_v, [ID_C \| AD_C \| ID_V])$$

8.List any 2 applications of X.509 Certificates. (NOV/DEC 2017)

- ❖ Document signing and Digital signature.
- ❖ Web server security with the help of Transport Layer Security (TLS)/Secure Sockets Layer (SSL) certificates.
- ❖ Email certificates.
- ❖ Code signing.
- ❖ Secure Shell Protocol (SSH) keys.
- ❖ Digital Identities.

9.How a digital signature differs from authentication protocols? (APRIL/MAY 18)

A (digital) signature is created with a private key, and verified with the corresponding public key of an asymmetric key-pair.

Only the holder of the private key can create this signature, and normally anyone knowing the public key can verify it.

Digital signatures don't prevent the replay attack mentioned previously

Authentication Protocols used **to convince parties of each other's identity** and to ***exchange session keys***.

Mutual Authentication

Protocols enable ***communicating parties to satisfy themselves mutually about each other's identity and to exchange session keys.***

Problem of authenticated key exchange

Problems to Key issues are

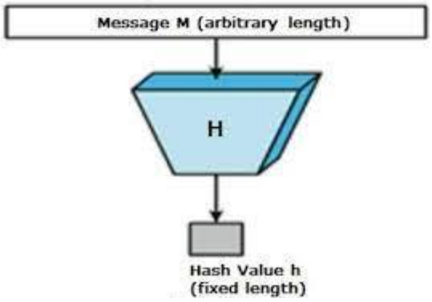
- **Confidentiality** – to protect session keys and prevent masqueraded(make believe) and compromised.
- **Timeliness** – to **prevent replay attacks**

10.What is a hash in cryptography?[Apr/May 2018]

Or

Define the term Message digest[Nov/Dec 2018]

Hashing is **the process of transforming any given value or a string of characters into another value**.
This is usually represented by a **shorter, fixed-length value or key** that represents and makes it easier to find or employ the original string.



11.What is Digital Signature[Nov/Dec 2018]

- A digital signature is an **authentication mechanism** that enables the sender of a message to **attach a code** that **acts as a signature**.
- Typically ***the signature*** is formed by **taking the hash of the message** and encrypting ***the message with the sender's private key.***

The **signature guarantees** the source and integrity of the message

12.Contrast various SHA algorithms[Nov/Dec 2018]

SHA-0: The original version of the 160-bit hash function published in 1993 under the name "SHA". It was withdrawn shortly after publication due to an undisclosed "significant flaw" and replaced by the slightly revised version SHA-1.

SHA-1: A 160-bit hash function which resembles the earlier MD5 algorithm. This was designed by the National Security Agency (NSA) to be part of the Digital Signature Algorithm.

SHA-2: A family of two similar hash functions, with different block sizes, known as SHA256 and SHA-512. SHA-256 uses 32-bit words where SHA-512 uses 64-bit words.

SHA-3: It supports the same hash lengths as SHA-2, and its internal structure differs significantly from the rest of the SHA family.

13.State the requirements of digital signature[Nov/Dec 2019]

- The signature must be a **bit pattern** that ***depends on the message being signed.*****[**Somewhat related to Message]
- The signature must use **some information unique to the sender**, to prevent both **forgery and denial.**
- It must be **relatively easy to produce** the digital signature.
- It must be **relatively easy to recognize and verify** the digital signature.[verification must be simpler]

- It must be **computationally infeasible to forge a digital signature**, either by **constructing a new message** for an **existing digital signature** or by constructing a fraudulent digital signature for a given message.
- It must be practical to **retain a copy of the digital signature** in storage.

14.Compare Direct and Arbitrated digital signature. (Understand) [NOV/DEC 19]

1. Direct Digital Signature:

- In a direct digital signature scheme, a user generates their own key pair: a private key for signing and a public key for verification.
- The user is responsible for securely managing their private key. If the private key is compromised, it could lead to unauthorized signature generation.
- The user can sign any document or message they want with their private key.
- Verification of the signature is done by using the corresponding public key.
- Direct digital signatures are suitable for applications where the user has full control over their keys and the signing process.

2. Arbitrated Digital Signature:

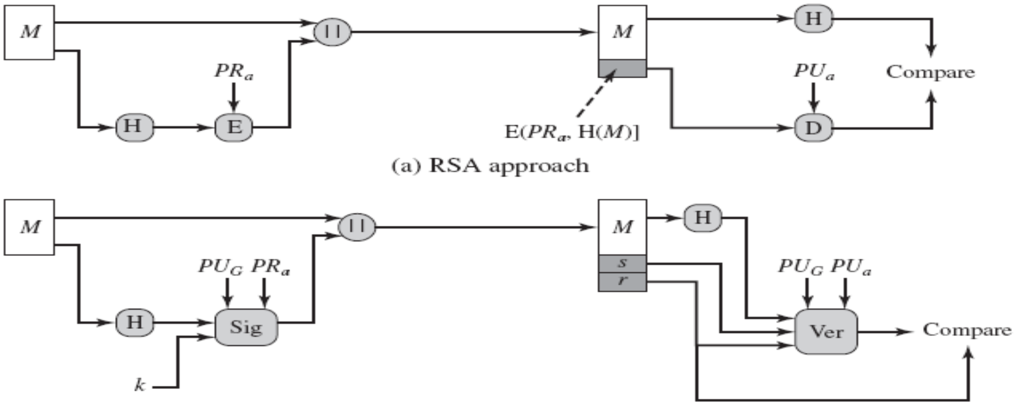
- In an arbitrated digital signature scheme, a trusted third party (arbiter) is involved in the signing process.
- The user generates a key pair as in the direct method, but they do not directly sign documents with their private key.
- Instead, the user sends the document and a request to the arbiter for signature.
- The arbiter reviews the request and the document and decides whether to grant the signature.
- If the arbiter approves, they sign the document on behalf of the user and return the signed document.
- Verification of the signature is done by using the arbiter's public key.
- Arbitrated digital signatures are suitable for situations where trust, control, or regulatory compliance is a significant concern.

15.What entities constitute a full service in Kerberos environment?

A full service environment consists of a

i) Kerberos server, ii) Number of clients, and iii) Number of application servers

16.Draw functional diagram of RSA and DSS based Digital signature?[Nov /Dec 2021]



(a) RSA approach

(b) DSS approach

17.Define Replay Attack[Nov 2011]

Replay Attacks

A ***valid signed message*** is copied and ***later resent***

Examples of replay attacks

(i)Simple replay :The **opponent** simply ***copies the message and replays*** it later.

(ii)Repetition that can be logged

The **opponent replay** a ***time stamped message*** within ***a valid time window***.

(iii)Repetition that cannot be detected

The attacker would have **suppressed the original message** from the receiver. Only the **replay message alone arrives**.

(iv)Backward replay without modification

This is a ***replay back to the message sender*** itself.This is possible only if ***the sender cannot easily recognize the difference between the message sent and the message received*** based on the content.

18.How is the security of MAC is expressed?[Nov/Dec 2017]

Computation resistance: [Mac value differs if **x ≠xi.]**

Given one or more text-MAC pairs (xi, C_K[xi_l]), it is computationally infeasible to compute any text-MAC pair (x, C_K(x)) **for any new input x ≠xi**

19. What do you mean by one way property in hash function? (APR/MAY 2011)(NOV/DEC 2012)

The one way property of hash function indicates that it is easy to generate a code given a message, but virtually impossible to generate a message given a code. This property is important if the authentication technique involves the use of a secret value.

- For any given value h, it is computationally infeasible to find x such that H(x) = h – one way property.
- For any given block x, it is computationally infeasible to find y ≠ x with H(y) = H(x) – weak collision resistance.
- It is computationally infeasible to find any pair (x, y) such that H(x) = H(y) – strong collision property

20. What are birthday attacks? (APR/MAY 2014)

If an encrypted 64 bit hash code C is transmitted with the corresponding unencrypted message M , then an opponent would need to find an M' such that H(M') = H(M)to substitute another message to substitute another message and fool the receiver. Thus the user has to try about 2^{63} combinations to find one that matches the hash code of the intercepted message. This is called as Birthday attack

PART - B

1.What is digital signature?Explain the key generation,signing and signature verification algorithm?Bring out the steps followed to create a digital signature[Nov/Dec 2022]

- Definition
- Generic model of digital signature process diagram
- Explain each step
- Required formulas for each steps
- Diagram for signing and verifying

2. Many websites requires users to register before they can access information or services.Suppose that you register at such as website but when you return later you have forgotten your password,The website then asks you to enter your email and address which you do.Later you receive your original password via email.Discuss several security concerns with this approach to deal with forgotten password.[Nov/Dec 2022]

Answer:

- ❖ Explain the steps need to taken
- ❖ Explain each steps and the process
- ❖ Explain security conerns related to the process

3. Briefly explain the steps of message digest generation in Whirlpool with a block diagram.[Nov/Dec 2020]

- ❖ Whirlpool Hash Structure
- ❖ Block Cipher W
- ❖ Performance of Whirlpool

4. Explain PKI management model and its operations with the help of a diagram.[Nov/Dec 2020]

- ❖ Explanation about PKIX
- ❖ PKIX Architectural Model Diagram

5.Discuss Client Server Mutual authentication, with example flow diagram. (NOV/DEC 2016)

Or

What is Kerberos ?Explain how it provides authenticated service.[Apr/May 2019]

Or

List the requirements of Kerberos[Nov 2021]

- ❖ Define Kerberos
- ❖ Requirements of Kerberos
- ❖ A simple authentication dialogue
- ❖ Using Authentication Server
- ❖ Diagram –Overview of Kerberos
- ❖ Using Ticket Granting Server
- ❖ Summary of Kerberos Message Exchange

6.Explain SHA512 in detail [Nov/Dec 2016]

Write steps involved in the generation of Message digest [Nov 2021]

Or

With a neat diagram.explain the steps involved SHA algorithm for encrypting a message with maximum length less than 2^{128} bits and produces as output a 512-bit message digest.

[Nov/Dec 2017]

Definition

Diagram -Message Digest Generation Using SHA-512

Processing Steps

Step 1 Append padding bits.

Step 2 Append length

Step 3 Initialize hash buffer

Step 4 Process message in 1024-bit (128-word) blocks

- Diagram SHA-512 Processing of a Single 1024 Bit Block
- Diagram Elementary SHA-512 Operation (single round)
- Diagram Creation of 80-word Input Sequence for SHA-512 Processing of Single Block

7.How Hash function algorithm is designed? Explain their features and properties [Apr/May 2018]

- Define hash function
- Block diagram of hash function
- Basic uses of Hash function
- Requirements of Hash Function
- Security of Hash function

8.Explain briefly about the certification mechanisms in X.509[Apr/May 2018]

- **Define X.509**
- **Diagram**
- **Public Key Certificate Use**
- **Obtaining a User's Certificate**
- **Revocation of certificates**

CS8792-CRYPTOGRAPHY AND NETWORK SECURITY

UNIT V SECURITY PRACTICE AND SYSTEM SECURITY 9

Electronic Mail security – PGP, S/MIME – IP security – Web Security - SYSTEM SECURITY: Intruders – Malicious software – viruses – Firewalls.

2 Marks

1.Why Email compatibility function in PGP required?[Nov/Dec 2022]

- Many electronic mail systems only permit the **use of blocks consisting of ASCII texts.**
- To accommodate this restriction, PGP provides the service of **converting the raw 8-bit binary stream to a stream of printable ASCII characters.**
- The scheme used for this purpose is **radix-64 conversion**.**Radix 64 conversion** is used to ***convert binary data into ASCII characters*.**
- e.g., consider the 24-bit (3 octets) raw text sequence . we can express this input in block of 6-bits to produce 4 ASCII characters.
- 001000 11 0101 110010 010001
- I L Y R => corresponding ASCII characters

2.Define virus.specify the types of viruses.[Nov/Dec 2022]

- A virus is **a piece of software** that can "infect" other programs by modifying them; **the modification includes a copy of the virus program**, which can then go on to infect other programs.
- A virus can do anything that **other programs do**. The only difference is that it **attaches itself to another program and executes** secretly when the host program is run.

Once a virus is executing, it can perform any function, such as **erasing files and programs.**

Types of virus

A virus classification **by target** includes the following categories:

• **Boot sector infector:** Infects a master boot record or boot record and spreads when a system is booted from the disk containing the virus.

• **File infector**: Infects files that the operating system or shell consider to be executable.

• **Macro virus**: Infects files with macro code that is interpreted by an applica1tion.

3. List out the applications of SSL.[Nov/Dec 2020]

(i)Secure Websites (HTTPS): SSL/TLS is most commonly used to secure websites through HTTPS (HTTP Secure

(ii)Email Encryption (SMTP/POP/IMAP): SSL/TLS can be used to secure email communication between email clients and servers. This is particularly important for protecting the confidentiality of email content and login credentials.

(iii)Virtual Private Networks (VPNs): SSL/TLS can be employed in VPNs to create secure and encrypted tunnels for remote access to corporate networks. It ensures that data transmitted between a user's device and the corporate network remains confidential and secure.

(iv)File Transfer (FTPS and SFTP): SSL/TLS is used in secure file transfer protocols like FTPS (FTP Secure) and SFTP (SSH File Transfer Protocol). It encrypts files during transmission, preventing unauthorized access to sensitive data.

Instant Messaging (IM): Some instant messaging services and clients use SSL/TLS to encrypt chat messages and protect user privacy.

4. What do you mean by IP Security policy?[Nov/Dec 2022]

Fundamental to the operation of IPsec is the concept of a security policy applied to each IP packet that transits from a source to a destination

IPsec policy is determined primarily by the interaction of two databases, the security association database (SAD) and the security policy database (SPD).

5. Explain the process of Radix 64 conversion[Nov/Dec 2021]

Radix 64 conversion is used to ***convert binary data into ASCII characters*.**

e.g., consider the 24-bit (3 octets) raw text sequence . we can express this input in block of 6-bits to produce 4 ASCII characters.

001000 11 0101 110010 010001

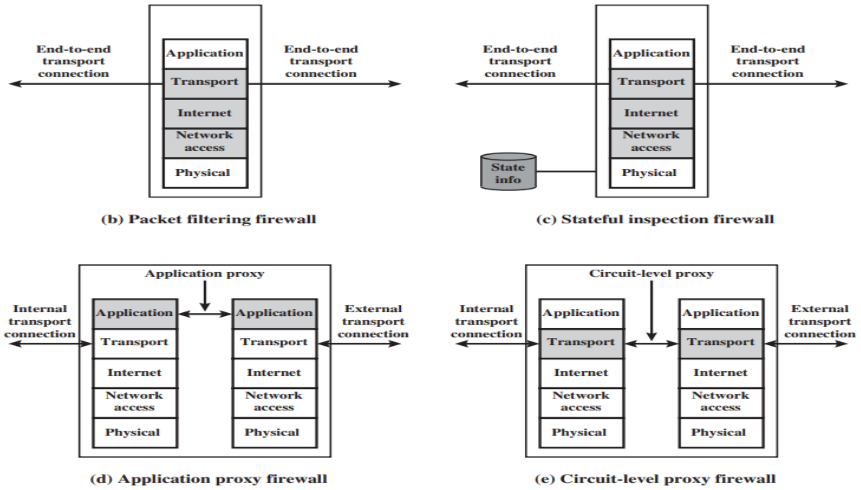
I L Y R => corresponding ASCII characters

6. Write short notes on Spammers and Key loggers.[Nov/Dec 2021,Apr/ May 2023]

Spammer programs Used to send large volumes of unwanted e-mail

Keyloggers Captures keystrokes on a compromised system

7.What are the various types of firewall?[Apr/May 2023]



(b) Packet filtering firewall

(c) Stateful inspection firewall

(d) Application proxy firewall

(e) Circuit-level proxy firewall

Figure Types of Firewalls

8.List the limitations of SMTP[Nov/Dec 2016]

1. ***SMTP cannot transmit executable files*** or ***other binary objects.***

2. *SMTP cannot transmit text data that includes national language* **characters** because these are represented by **8-bit codes** with values of **128 decimal or higher**, and **SMTP is limited to 7-bit ASCII.**

3. **SMTP servers** may **reject mail message** over **a certain size**.

4. **SMTP gateways** that translate ***between ASCII and the character code EBCDIC*** do not use a *consistent set of mappings*, resulting in ***translation problems***.

5. SMTP gateways to ***X.400 electronic mail networks*** cannot handle ***nontextual data*** included in ***X.400 messages***.

6. Some SMTP implementations ***do not adhere completely to the SMTP standards*** defined in **RFC 821**. Common problems include:

- Deletion, addition, or reordering of carriage return and linefeed
- Truncating or wrapping lines longer than 76 characters
- Removal of trailing white space (tab and space characters)
- Padding of lines in a message to the same length
- Conversion of tab characters into multiple space characters

9. List out the services provided by PGP.

The ***actual operation of PGP***, as opposed to the management of keys, consists of five services: **(i)** ***authentication, (ii)confidentiality, (iii)compression, and (iv)e-mail compatibility(v)Segmentation [2 Marks]***

10.What do you mean by PGP?

- PGP is **an open-source, freely available software package** for e-mail security.
- It provides

(i)**authentication through tthe use of digital signature**,
(ii)**confidentiality** through the use of **symmetric block encryption**, (iii)compression using the **ZIP algorithm**, and
(iv)**e-mail compatibility using the radix-64 encoding scheme**.

11.Define MIME Header

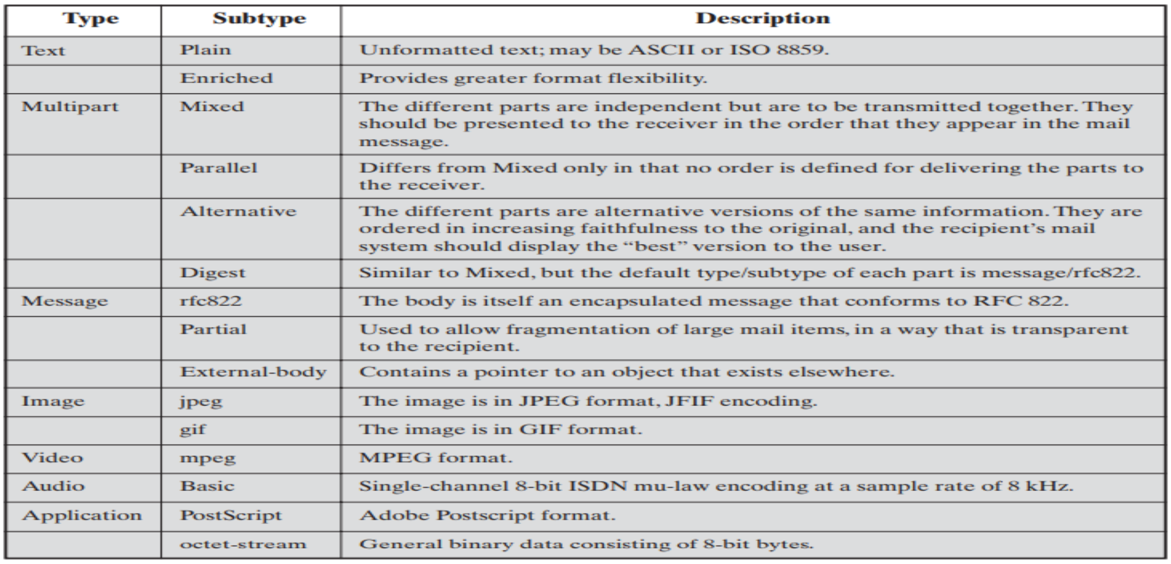
The five header fields defined in MIME are as follows:

- **MIME-Version**: Must have the parameter **value 1.0**. This field indicates that the message conforms to RFCs 2045 and 2046.
- **Content-Type**: Describes **the data contained in the body** with sufficient detail
- **Content-Transfer-Encoding**: Indicates **the type of transformation** that has been used to represent the body of the message in a way that is acceptable for mail transport.

- **Content-ID:** Used to identify the message.
- **Content-Description**: A text description of the object with the body; this is useful when the object is not readable (e.g., audio data).

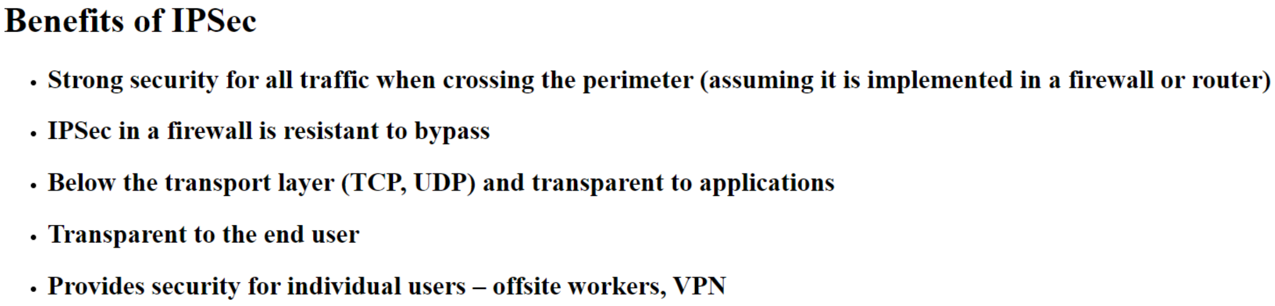
12.List of types of MIME

MIME Content Types



Type	Subtype	Description
Text	Plain	Unformatted text; may be ASCII or ISO 8859.
	Enriched	Provides greater format flexibility.
Multipart	Mixed	The different parts are independent but are to be transmitted together. They should be presented to the receiver in the order that they appear in the mail message.
	Parallel	Differs from Mixed only in that no order is defined for delivering the parts to the receiver.
	Alternative	The different parts are alternative versions of the same information. They are ordered in increasing faithfulness to the original, and the recipient's mail system should display the "best" version to the user.
	Digest	Similar to Mixed, but the default type/subtype of each part is message/rfc822.
Message	rfc822	The body is itself an encapsulated message that conforms to RFC 822.
	Partial	Used to allow fragmentation of large mail items, in a way that is transparent to the recipient.
	External-body	Contains a pointer to an object that exists elsewhere.
Image	jpeg	The image is in JPEG format, JFIF encoding.
	gif	The image is in GIF format.
Video	mpeg	MPEG format.
Audio	Basic	Single-channel 8-bit ISDN mu-law encoding at a sample rate of 8 kHz.
Application	PostScript	Adobe Postscript format.
	octet-stream	General binary data consisting of 8-bit bytes.

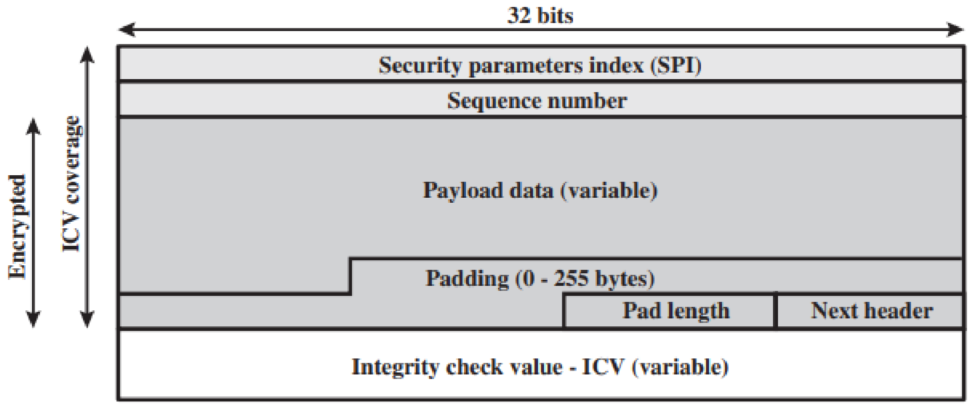
13.Specify the benefits of IPSec.



Benefits of IPSec

- Strong security for all traffic when crossing the perimeter (assuming it is implemented in a firewall or router)
- IPSec in a firewall is resistant to bypass
- Below the transport layer (TCP, UDP) and transparent to applications
- Transparent to the end user
- Provides security for individual users – offsite workers, VPN

14.Draw the ESP packet format



(a) Top-level format of an ESP Packet

15.Differentiate transport and tunnel mode in IPSec

Transport Mode	**Tunnel Mode**
It provides protection for upper layer protocols	It provides protection to the entire Ip packet
d-to-end communication between two host.	It is used when one or both ends of an SA is a security gateway,such as firewall or router that implement IpSec.
uthentication IP payload and selected portions header and IPV6 extension header	Authenticates entire inner IP packet plus selected portions of outer IP header and outer IPV6 extension headers.

16.List the three classes of Intruders.

Three classes of intruders are as follows:

Masquerader – an ***<u>individual who is not authorized</u>*** to use **the computer** and ***who penetrates a system's access controls*** to exploit **a legitimate user's account**.

Misfeasor – a **legitimate user** who accesses **data, programs, or resources** for which such **access is not authorized**, or who is authorized for such access but **misuse his or her privileges**.

Clandestine user – an individual who ***<u>seizes supervisory control of the system</u>*** and uses this ***control to avoid(escape from) auditing*** and ***<u>access controls or to suppress audit collection.</u>***

17.What is an Intruder

Intruders are the attackers who attempt to breach the security of a network

18.Define Worm

Worm is a program that can **replicate itself and send copies from computer to computer across** network connections.

Upon arrival, the worm may be activated to replicate and propagate again. In addition to propagation, the worm usually performs some unwanted function.

Example

Morris worm ,Email Worms

- ❖ Email Worms spread through malicious email as an attachment or a link of a malicious website.

- ❖ Instant Messaging Worms: Instant Messaging Worms spread by sending links to the contact list of instant messaging applications such as Messenger, WhatsApp, Skype, etc.
- ❖ The Morris worm was designed to spread on UNIX systems and used a number of different techniques for propagation

19.Define Zombie

Zombie A ***<u>program that secretly takes over another Internet-attached computer</u>*** and then uses that computer to **launch attacks** that are difficult to trace to the zombie's creator.

20.Define Malicious software

The software which is used for ***<u>destructive purpose</u>*** .It leads to the destruction process.It is called malware.

The most sophisticated types of threats to computer systems are presented by programs that exploit vulnerabilities in computing systems.

21.What are the effects of malicious software write any two?

Malware impacts your computer in the following ways: **Disrupts operations. Steals sensitive information. Allows unauthorized access to system resources**.

22.Discriminate statistical anomaly detection and rule based detection

Approaches to Intrusion Detection

Statistical Anomaly Detection

- ❖ Threshold based Detection
    - o Count occurrences of specific event over time
    - o Ineffective Detector
- ❖ Profile Based
    - o Characterize past behaviour of users
    - o Detect significant deviations

Rule Based Detection

- ❖ Anomaly
    - o Observe events on system and apply rules to decide if activity is suspicious or not
- ❖ Penetration identification
- o Analyse historical audit records to identify usage patterns & auto generate rules for them.
- o It does not require prior knowledge of security flaws

23.Define Honeypot

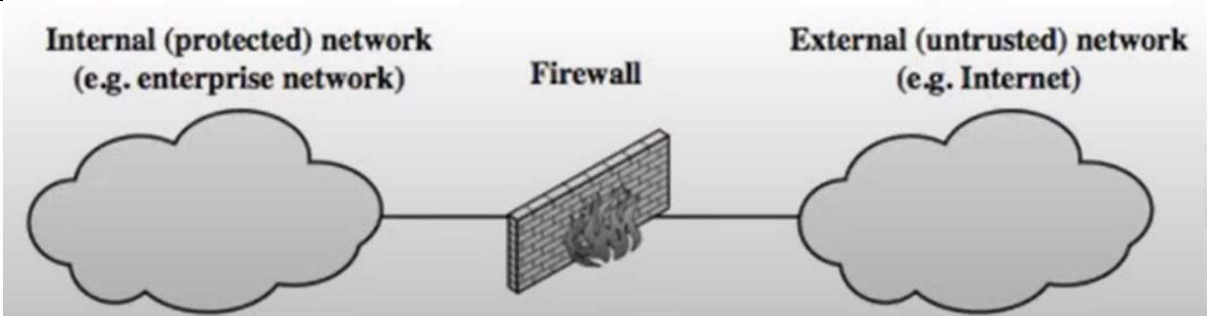
Definition

Honeypots are decoy(tricky) systems that are designed to lure a potential attacker away from critical systems. Honeypots are designed to

- ➢ Divert an attacker from accessing critical systems
- ➢ **Collect information** about the attacker's activity
- ➢ Encourage the attacker to stay on the system long enough for administrators to respond

24.Define the role of firewall

- ➢ A Firewall is a network security system that **monitors and filters incoming and outgoing network traffic** based on ***predetermined security* rules**.


Internal (protected) network
(e.g. enterprise network)
Firewall
External (untrusted) network
(e.g. Internet)

- A Firewall is a network security device that **monitors and filters incoming and outgoing network traffic based on an organization's previously established security policies**.

25.What are the two functions of a firewall?

- A firewall is a protective measure that safeguards an individual's or company's computer network. It provides two basic security functions, including **packet filtering, which inspects traffic at the packet level, and acting as an application proxy, providing security measures at the application level**.

26.List the Types of Firewall

- Packet Filtering Firewall
- Stateful inspection firewall
- Application proxy firewall
- Circuit-level proxy firewall

27.List the design goals of firewalls

- All traffic **from inside to outside**, and **vice versa**, must pass through the firewall.This is achieved by **physically blocking all access** to the **local network** except via the firewall**.**
- Only **authorized traffic**, as ***defined by the local security policy***, will be allowed **to pass**. Various types of firewalls are used, which implement **various types of security policie**
- The **firewall itself is immune to penetration**.This implies **the use of a hardened system with a secured operating system**.
- **Trusted computer systems** are suitable **for hosting a firewall** and often required in government applications.

Part B

1.Discuss the seven types of MIME content type.[Nov/Dec 2021]

- **MIME content types table**

2.With the help of a neat diagram, explain wired and wireless TLS architecture.[Nov/Dec 2020]

Wireless TLS

WTLS Protocol Architecture

WTLS Protocol Stack Diagram

WTLS Record Protocol operation Diagram

Wired TLS

WAP2 end to end security approaches diagram

3.Illustrate how PGP encryption is implemented through a suitable diagram.

- Define PGP
- PGP Message Generation with Diagram

4.How does PGP provides confidentiality and authentication service for e-mail and file storage applications?Draw the block diagram and explain its components[Nov/Dec 2020]

- PGP cryptographic Functions Block Diagram
- Explanation

5.Explain about S/MIME in detail

- Define MIME Types
- S/MIME Functionality or S/MIME Functions

6.Explain IP Security Architecture in detail

- Define IP Security
- Explain all the components
- Draw Architecture Diagram

7.Explain Encapsulating Security Payload In Detail

ESP Format Diagram

- Encryption and Authentication Algorithms
- Padding
- Anti-Replay Service
- Transport and Tunnel Modes

8.Explain the characteristics and types of firewall?

- Goals of firewall
- General techniques of firewall
- Scope of firewall

Types

- Packet Filtering Firewall
- Statefull Inspection firewall
- Application proxy firewall
- Circuit level proxy firewall

9.Explain WebSecurity in Detail

- Definition
- Web security considerations or How to Secure the Web Site
- Updated Softwares
- Beware of SQL injection
- Cross Site Scripting (XSS)
- Error Message
- Data Validation
- Passwords
- Web Security Threats
- Web Traffic Security Approaches