notes click

1. What is cryptanalysis and cryptography?

   Cryptography which focuses on creating secret codes and **Cryptanalysis** which is the study of the cryptographic algorithm and the breaking of those secret codes.

   The person practicing Cryptanalysis is called a **Cryptanalyst**.

   It helps us to better understand the cryptosystems and also helps us improve the system by finding any weak point and thus work on the algorithm to create a more secure secret code.

   For example, a Cryptanalyst might try to decipher a ciphertext to derive the plaintext. It can help us to deduce the plaintext or the encryption key.

2. What are the types of attacks on encrypted message?

Brute force attack

Public and private keys play a significant role in encrypting and decrypting the data in a cryptographic system. In a brute force attack, the cybercriminal tries various private keys to decipher an encrypted message or data. If the key size is 8-bit, the possible keys will be 256 (i.e., 28). The cybercriminal must know the algorithm (usually found as open-source programs) to try all the 256 possible keys in this attack technique.

Ciphertext-only attack

In this attack vector, the attacker gains access to a collection of ciphertext. Although the attacker cannot access the plaintext, they can successfully determine the ciphertext from the collection. Through this attack technique, the attacker can occasionally determine the key.

Chosen plaintext attack

In this attack model, the cybercriminal can choose arbitrary plaintext data to obtain the ciphertext. It simplifies the attacker's task of resolving the encryption key. One well-known example of this type of attack is the differential cryptanalysis performed on block ciphers.

Chosen ciphertext attack

In this attack model, the cybercriminal analyzes a chosen ciphertext corresponding to its plaintext. The attacker tries to obtain a secret key or the details about the system. By analyzing the chosen ciphertext and relating it to the plaintext, the attacker attempts to guess the key. Older versions of RSA encryption were prone to this attack.

Known plaintext attack

In this attack technique, the cybercriminal finds or knows the plaintext of some portions of the ciphertext using information gathering techniques. Linear cryptanalysis in block cipher is one such example.

Key and algorithm attack

notes click

Here, the attacker tries to recover the key used to encrypt or decrypt the data by analyzing the cryptographic algo

3. What are the key principles of security?

The basic tenets of information security are confidentiality, integrity and availability. Every element of the information security program must be designed to implement one or more of these principles. Together they are called the CIA Triad.

Confidentiality

Confidentiality measures are designed to prevent unauthorized disclosure of information. The purpose of the confidentiality principle is to keep personal information private and to ensure that it is visible and accessible only to those individuals who own it or need it to perform their organizational functions.

Integrity

Consistency includes protection against unauthorized changes (additions, deletions, alterations, etc.) to data. The principle of integrity ensures that data is accurate and reliable and is not modified incorrectly, whether accidentally or maliciously.

Availability

Availability is the protection of a system's ability to make software systems and data fully available when a user needs it (or at a specified time). The purpose of availability is to make the technology infrastructure, the applications and the data available when they are needed for an organizational process or for an organization's customers.

4. Compare Substitution and Transposition techniques with Example.

S.NO	Substitution Cipher Technique	Transposition Cipher Technique
1.	In substitution Cipher Technique, plain text characters are replaced with other characters, numbers and symbols.	In transposition Cipher Technique, plain text characters are rearranged with respect to the position.
2.	Substitution Cipher's forms are: Mono alphabetic substitution cipher and poly alphabetic substitution cipher.	Transposition Cipher's forms are: Key-less transposition cipher and keyed transposition cipher.
3.	In substitution Cipher Technique, character's identity is changed while its position remains unchanged.	While in transposition Cipher Technique, The position of the character is changed but character's identity is not changed.
4.	In substitution Cipher Technique, The letter with low frequency can detect plain text.	While in transposition Cipher Technique, The Keys which are nearer to correct key can disclose plain text.
5.	The example of substitution Cipher is Caesar Cipher.	The example of transposition Cipher is Rail Fence Cipher.

notes click

5. What is Caesar cipher? How to Encrypt a massage “Cryptography” with key 3 using Caesar
cipher?

The Caesar cipher is the simplest and oldest method of cryptography. The Caesar cipher method is based on a mono-alphabetic cipher and is also called a shift cipher or additive cipher. Julius Caesar used the shift cipher (additive cipher) technique to communicate with his officers. For this reason, the shift cipher technique is called the Caesar cipher. The Caesar cipher is a kind of replacement (substitution) cipher, where all letter of plain text is replaced by another letter.

Let's take an example to understand the Caesar cipher, suppose we are shifting with 1, then A will be replaced by B, B will be replaced by C, C will be replaced by D, D will be replaced by C, and this process continues until the entire plain text is finished.

Caesar ciphers is a weak method of cryptography. It can be easily hacked. It means the message encrypted by this method can be easily decrypted.

for key=3,cipher test= Fubswrjudskb

6. How does simple columnar transposition work?

Given a plain-text message and a numeric key, cipher/de-cipher the given text using Columnar Transposition Cipher

The Columnar Transposition Cipher is a form of transposition cipher just like Rail Fence Cipher. Columnar Transposition involves writing the plaintext out in rows, and then reading the ciphertext off in columns one by one.

Encryption

```
Input : Geeks for Geeks
Key = HACK
Output : e  kefGsGsrekoe_
```

Decryption

```
Input : e  kefGsGsrekoe_
Key = HACK
Output : Geeks for Geeks
```

[notes click]

Encryption

Given text = Geeks for Geeks
Keyword = HACK **Length of Keyword** = 4 (no of rows) **Order of Alphabets in HACK** = 3124

H	A	C	K
3	1	2	4
G	e	e	k
s	_	f	o
r	_	G	e
e	k	s	_

Print Characters of column 1,2,3,4
Encrypted Text = e kefGsGsrekoe_

7. What is Monoalphabetic cipher? How it is different from Polyalphabetic cipher?

1. Monoalphabetic Cipher :

A monoalphabetic cipher is any cipher in which the letters of the plain text are mapped to cipher text letters based on a single alphabetic key. Examples of monoalphabetic ciphers would include the Caesar-shift cipher, where each letter is shifted based on a numeric key, and the atbash cipher, where each letter is mapped to the letter symmetric to it about the center of the alphabet.

2. Polyalphabetic Cipher :

A polyalphabetic cipher is any cipher based on substitution, using multiple substitution alphabets. The Vigenère cipher is probably the best-known example of a polyalphabetic cipher, though it is a simplified special case.

SR.NO	Monoalphabetic Cipher	Polyalphabetic Cipher
1	Monoalphabetic cipher is one where each symbol in plain text is mapped to a fixed symbol in cipher text.	Polyalphabetic cipher is any cipher based on substitution, using multiple substitution alphabets.
2	The relationship between a character in the plain text and the characters in the cipher text is one-to-one.	The relationship between a character in the plain text and the characters in the cipher text is one-to-many.
3	Each alphabetic character of plain text is mapped onto a unique alphabetic character of a cipher text.	Each alphabetic character of plain text can be mapped onto ‘m’ alphabetic characters of a cipher text.
4	A stream cipher is a monoalphabetic cipher if the value of key does not	A stream cipher is a polyalphabetic cipher if the value of key does depend

notes click

SR.NO	Monoalphabetic Cipher	Polyalphabetic Cipher
	depend on the position of the plain text character in the plain text stream.	on the position of the plain text character in the plain text stream.
5	It includes additive, multiplicative, affine and monoalphabetic substitution cipher.	It includes autokey, Playfair, Vigenere, Hill, one-time pad, rotor, and Enigma cipher.
6	It is a simple substitution cipher.	It is multiple substitutions cipher.
7	Monoalphabetic Cipher is described as a substitution cipher in which the same fixed mappings from plain text to cipher letters across the entire text are used.	Polyalphabetic Cipher is described as substitution cipher in which plain text letters in different positions are enciphered using different cryptoalphabets.
8	Monoalphabetic ciphers are not that strong as compared to polyalphabetic cipher.	Polyalphabetic ciphers are much stronger.

8. Compare stream cipher and block cipher with example.

S.NO	Block Cipher	Stream Cipher
1.	Block Cipher Converts the plain text into cipher text by taking plain text's block at a time.	Stream Cipher Converts the plain text into cipher text by taking 1 byte of plain text at a time.
2.	Block cipher uses either 64 bits or more than 64 bits.	While stream cipher uses 8 bits.
3.	The complexity of block cipher is simple.	While stream cipher is more complex.
4.	Block cipher Uses confusion as well as diffusion.	While stream cipher uses only confusion.
5.	In block cipher, reverse encrypted text is hard.	While in-stream cipher, reverse encrypted text is easy.
6.	The algorithm modes which are used in block cipher are ECB (Electronic Code Book) and CBC (Cipher Block Chaining).	The algorithm modes which are used in stream cipher are CFB (Cipher Feedback) and OFB (Output Feedback).
7.	Block cipher works on transposition techniques like rail-fence technique, columnar transposition technique, etc.	While stream cipher works on substitution techniques like Caesar cipher, polygram substitution cipher, etc.
8.	Block cipher is slow as compared to a stream cipher.	While stream cipher is fast in comparison to block cipher.

9. Compare Substitution and Transposition techniques.

notes click

S.NO	Substitution Cipher Technique	Transposition Cipher Technique
1.	In substitution Cipher Technique, plain text characters are replaced with other characters, numbers and symbols.	In transposition Cipher Technique, plain text characters are rearranged with respect to the position.
2.	Substitution Cipher's forms are: Mono alphabetic substitution cipher and poly alphabetic substitution cipher.	Transposition Cipher's forms are: Key-less transposition cipher and keyed transposition cipher.
3.	In substitution Cipher Technique, character's identity is changed while its position remains unchanged.	While in transposition Cipher Technique, The position of the character is changed but character's identity is not changed.
4.	In substitution Cipher Technique, The letter with low frequency can detect plain text.	While in transposition Cipher Technique, The Keys which are nearer to correct key can disclose plain text.
5.	The example of substitution Cipher is Caesar Cipher.	The example of transposition Cipher is Rail Fence Cipher.

10. What is the difference between diffusion and confusion?

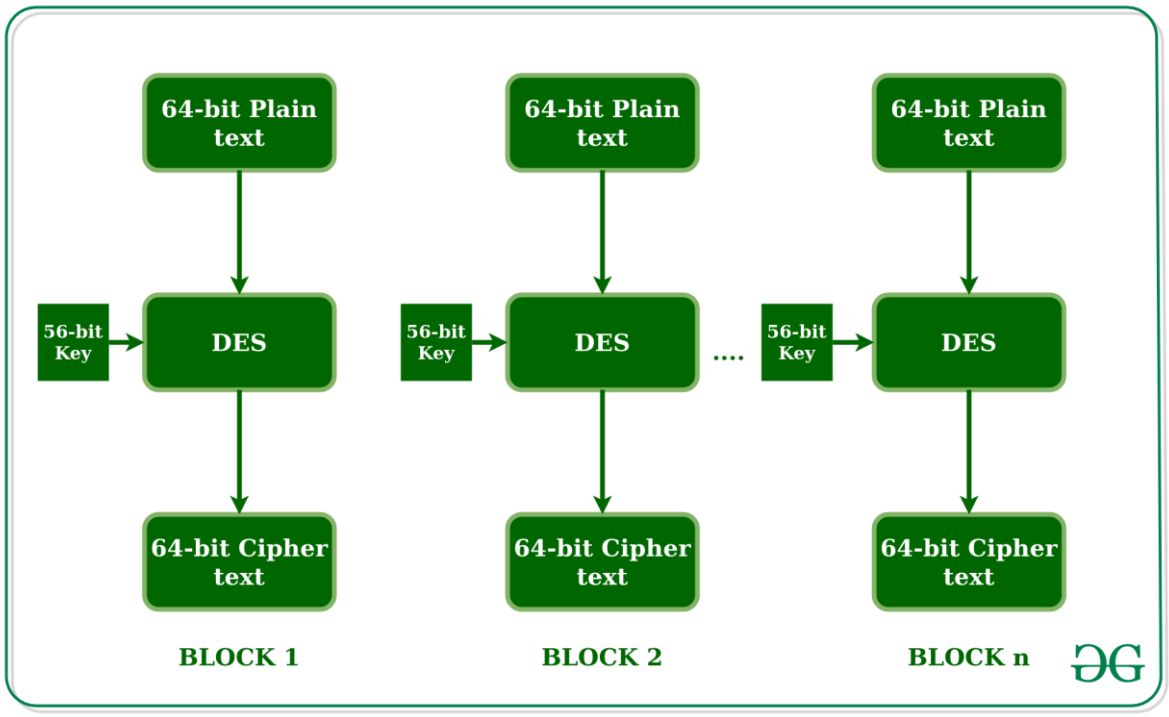
S.NO	Confusion	Diffusion
1.	Confusion is a cryptographic technique which is used to create faint cipher texts.	While diffusion is used to create cryptic plain texts.
2.	This technique is possible through substitution algorithm.	While it is possible through transportation algorithm.
3.	In confusion, if one bit within the secret's modified, most or all bits within the cipher text also will be modified.	While in diffusion, if one image within the plain text is modified, many or all image within the cipher text also will be modified
4.	In confusion, vagueness is increased in resultant.	While in diffusion, redundancy is increased in resultant.
5.	Both stream cipher and block cipher uses confusion.	Only block cipher uses diffusion.
6.	The relation between the cipher text and the key is masked by confusion.	While The relation between the cipher text and the plain text is masked by diffusion.

Confusion = **Substitution**
a --> b
Caesar Cipher

Diffusion = **Transposition or Permutation**
abcd --> dacb
DES

11. How many keys are required for two people to communicate via a cipher?
    one key
12. Draw the general structure of DES and explain the encryption decryption process.
    Data encryption standard (DES) has been found vulnerable to very powerful attacks and therefore, the popularity of DES has been found slightly on the decline. DES is a block cipher and encrypts data in blocks of size of **64 bits** each, which means 64 bits

of plain text go as the input to DES, which produces 64 bits of ciphertext. The same algorithm and key are used for encryption and decryption, with minor differences. The key length is **56 bits**. The basic idea is shown in the figure:



We have mentioned that DES uses a 56-bit key. Actually, the initial key consists of 64 bits. However, before the DES process even starts, every 8th bit of the key is discarded to produce a 56-bit key. That is bit positions 8, 16, 24, 32, 40, 48, 56, and 64 are discarded.

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	26	27	28	29	30	31	32
33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48
49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64

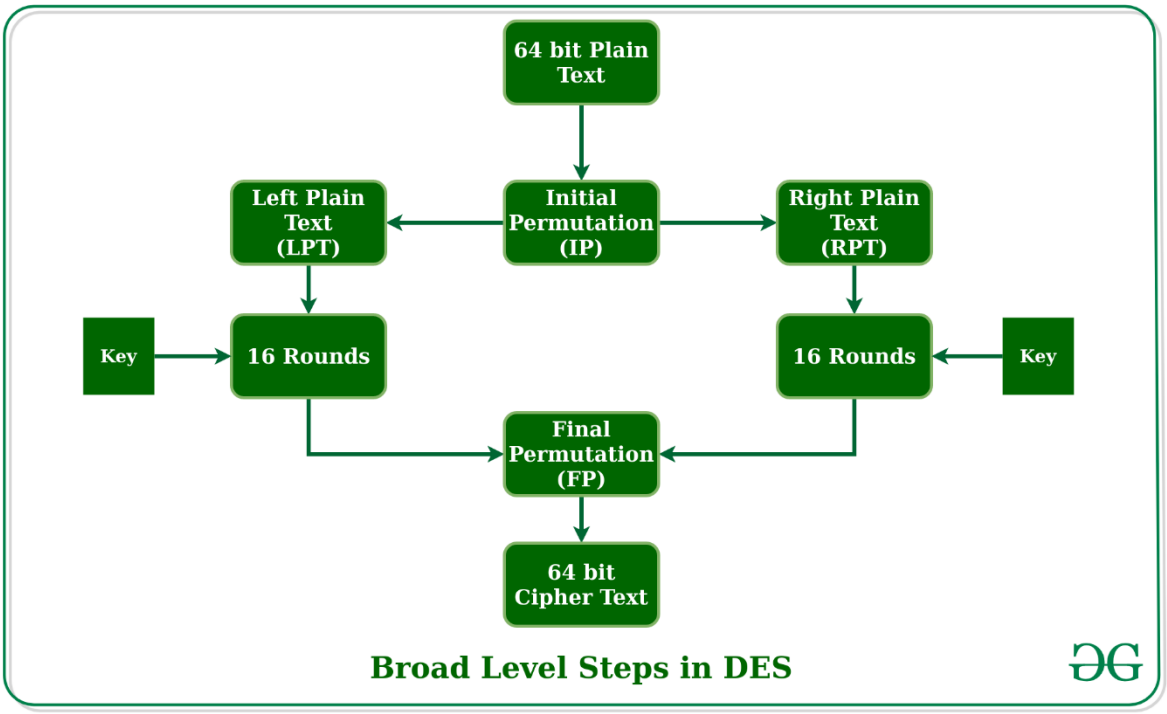
Figure - discording of every 8th bit of original key

Thus, the discarding of every 8th bit of the key produces a **56-bit key** from the original **64-bit key**.

DES is based on the two fundamental attributes of cryptography: substitution (also called confusion) and transposition (also called diffusion). DES consists of 16 steps, each of which is called a round. Each round performs the steps of substitution and transposition. Let us now discuss the broad-level steps in DES.

- In the first step, the 64-bit plain text block is handed over to an initial Permutation (IP) function.
- The initial permutation is performed on plain text.
- Next, the initial permutation (IP) produces two halves of the permuted block; saying Left Plain Text (LPT) and Right Plain Text (RPT).
- Now each LPT and RPT go through 16 rounds of the encryption process.
- In the end, LPT and RPT are rejoined and a Final Permutation (FP) is performed on the combined block
- The result of this process produces 64-bit ciphertext.

[notes click]



Initial Permutation (IP):

As we have noted, the initial permutation (IP) happens only once and it happens before the first round. It suggests how the transposition in IP should proceed, as shown in the figure. For example, it says that the IP replaces the first bit of the original plain text block with the 58th bit of the original plain text, the second bit with the 50th bit of the original plain text block, and so on.

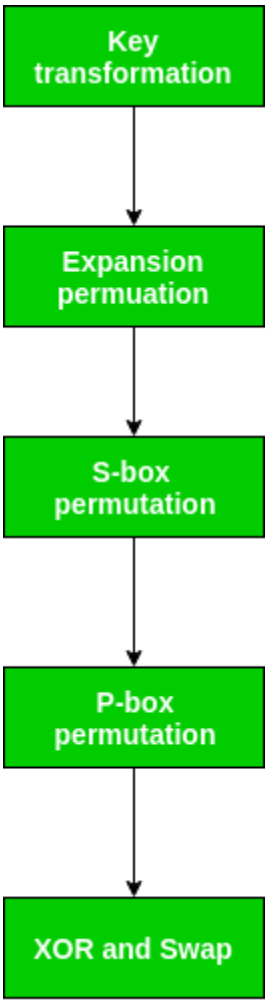
This is nothing but jugglery of bit positions of the original plain text block. the same rule applies to all the other bit positions shown in the figure.

58	50	42	34	26	18	10	2	60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6	64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1	59	51	43	35	27	19	11	3
61	33	45	37	29	21	13	5	63	55	47	39	31	23	15	7

Figure - Initial permutation table

As we have noted after IP is done, the resulting 64-bit permuted text block is divided into two half blocks. Each half-block consists of 32 bits, and each of the 16 rounds, in turn, consists of the broad-level steps outlined in the figure.

[notes click]



Step-1: Key transformation:

We have noted initial 64-bit key is transformed into a 56-bit key by discarding every 8th bit of the initial key. Thus, for each a 56-bit key is available. From this 56-bit key, a different 48-bit Sub Key is generated during each round using a process called key transformation. For this, the 56-bit key is divided into two halves, each of 28 bits. These halves are circularly shifted left by one or two positions, depending on the round.

For example: if the round numbers 1, 2, 9, or 16 the shift is done by only one position for other rounds, the circular shift is done by two positions. The number of key bits shifted per round is shown in the figure.

Round	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
#key bits shifted	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

Figure - number of key bits shifted per round

After an appropriate shift, 48 of the 56 bits are selected. for selecting 48 of the 56 bits the table is shown in the figure given below. For instance, after the shift, bit number 14 moves to the first position, bit number 17 moves to the second position, and so on. If we observe the table carefully, we will realize that it contains only 48-bit positions. Bit number 18 is discarded (we will not find it in the table), like 7 others, to reduce a 56-bit key to a 48-bit key. Since the key transformation process involves permutation as well as a selection of a 48-bit subset of the original 56-bit key it is called Compression Permutation.

notes click

14	17	11	24	1	5	3	28	15	6	21	10
23	19	12	4	26	8	16	7	27	20	13	2
41	52	31	37	47	55	30	40	51	45	33	48
44	49	39	56	34	53	46	42	50	36	29	32

Figure - compression permutation

Because of this compression permutation technique, a different subset of key bits is used in each round. That makes DES not easy to crack.

Step-2: Expansion Permutation:

Recall that after the initial permutation, we had two 32-bit plain text areas called Left Plain Text(LPT) and Right Plain Text(RPT). During the expansion permutation, the RPT is expanded from 32 bits to 48 bits. Bits are permuted as well hence called expansion permutation. This happens as the 32-bit RPT is divided into 8 blocks, with each block consisting of 4 bits. Then, each 4-bit block of the previous step is then expanded to a corresponding 6-bit block, i.e., per 4-bit block, 2 more bits are added.

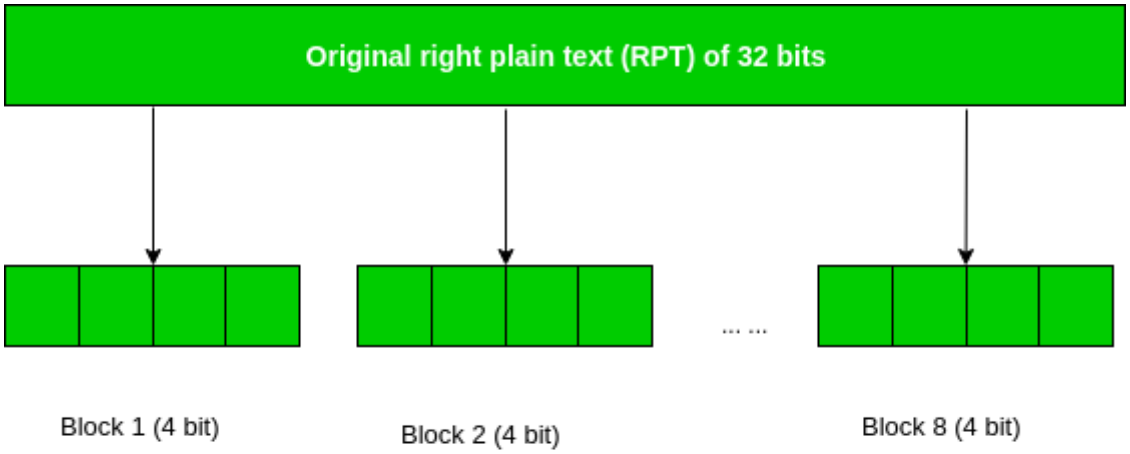


Figure - division of 32 bit RPT into 8 bit blocks

This process results in expansion as well as a permutation of the input bit while creating output. The key transformation process compresses the 56-bit key to 48 bits. Then the expansion permutation process expands the **32-bit RPT** to **48-bits**. Now the 48-bit key is XOR with 48-bit RPT and the resulting output is given to the next step, which is the **S-Box substitution**.

13. What is AES? Draw the general structure of AES and explain the encryption decryption process.

Advanced Encryption Standard (AES) is a specification for the encryption of electronic data established by the U.S National Institute of Standards and Technology (NIST) in 2001. AES is widely used today as it is a much stronger than DES and triple DES despite being harder to implement.

notes click

Points to remember

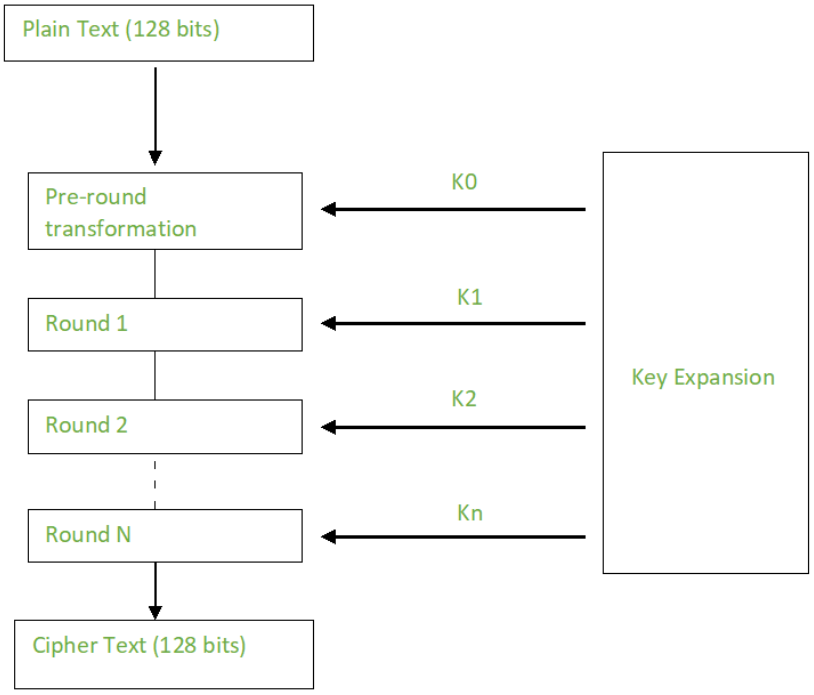
- AES is a block cipher.
- The key size can be 128/192/256 bits.
- Encrypts data in blocks of 128 bits each.

That means it takes 128 bits as input and outputs 128 bits of encrypted cipher text as output. AES relies on substitution-permutation network principle which means it is performed using a series of linked operations which involves replacing and shuffling of the input data.

Working of the cipher :
AES performs operations on bytes of data rather than in bits. Since the block size is 128 bits, the cipher processes 128 bits (or 16 bytes) of the input data at a time.
he number of rounds depends on the key length as follows :

- 128 bit key – 10 rounds
- 192 bit key – 12 rounds
- 256 bit key – 14 rounds

Creation of Round keys :
A Key Schedule algorithm is used to calculate all the round keys from the key. So the initial key is used to create many different round keys which will be used in the corresponding round of the encryption.



Encryption :
AES considers each block as a 16 byte (4 byte x 4 byte = 128) grid in a column major arrangement.
[b0 | b4 | b8 | b12 |
| b1 | b5 | b9 | b13 |
| b2 | b6 | b10| b14 |
| b3 | b7 | b11| b15]
Each round comprises of 4 steps :

notes click

- SubBytes
- ShiftRows
- MixColumns
- Add Round Key

The last round doesn't have the MixColumns round.

The SubBytes does the substitution and ShiftRows and MixColumns performs the permutation in the algorithm.

SubBytes :
This step implements the substitution.
In this step each byte is substituted by another byte. Its performed using a lookup table also called the S-box. This substitution is done in a way that a byte is never substituted by itself and also not substituted by another byte which is a compliment of the current byte. The result of this step is a 16 byte (4 x 4) matrix like before.

The next two steps implement the permutation.

ShiftRows :
This step is just as it sounds. Each row is shifted a particular number of times.

- The first row is not shifted
- The second row is shifted once to the left.
- The third row is shifted twice to the left.
- The fourth row is shifted thrice to the left.

(A left circular shift is performed.)

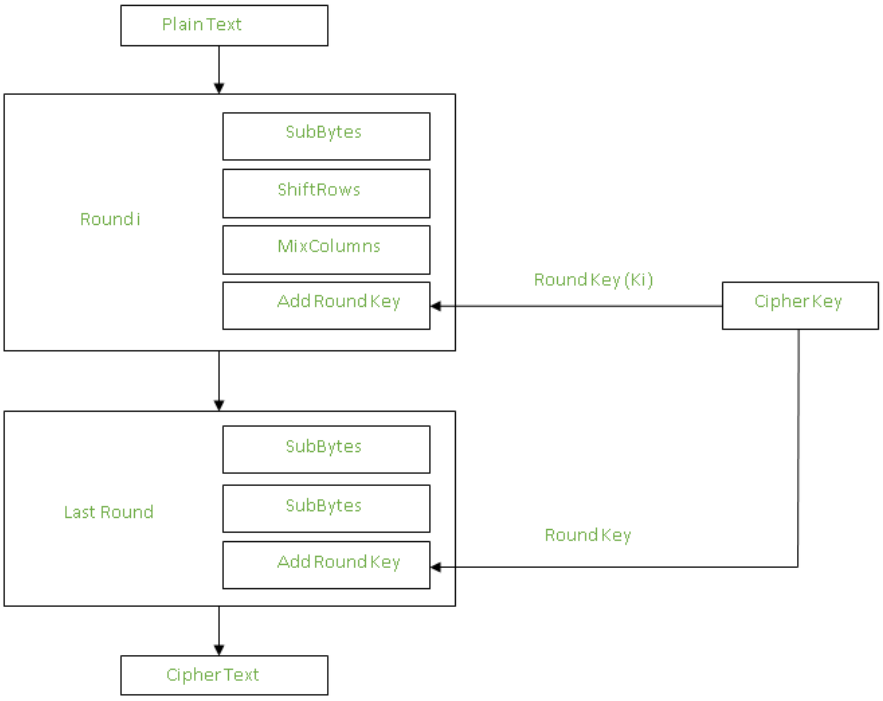
[b0 | b1 | b2 | b3] [b0 | b1 | b2 | b3]
| b4 | b5 | b6 | b7 | -> | b5 | b6 | b7 | b4 |
| b8 | b9 | b10 | b11 | | b10 | b11 | b8 | b9 |
[b12 | b13 | b14 | b15] [b15 | b12 | b13 | b14]

MixColumns :
This step is basically a matrix multiplication. Each column is multiplied with a specific matrix and thus the position of each byte in the column is changed as a result.
This step is skipped in the last round.

[c0] [2 3 1 1] [b0]
| c1 | = | 1 2 3 1 | | b1 |
| c2 | | 1 1 2 3 | | b2 |
[c3] [3 1 1 2] [b3]

Add Round Keys :
Now the resultant output of the previous stage is XOR-ed with the corresponding round key. Here, the 16 bytes is not considered as a grid but just as 128 bits of data.

[notes click]



After all these rounds 128 bits of encrypted data is given back as output. This process is repeated until all the data to be encrypted undergoes this process.

Decryption :
The stages in the rounds can be easily undone as these stages have an opposite to it which when performed reverts the changes.Each 128 blocks goes through the 10,12 or 14 rounds depending on the key size.
The stages of each round in decryption is as follows :

- Add round key
- Inverse MixColumns
- ShiftRows
- Inverse SubByte

The decryption process is the encryption process done in reverse so i will explain the steps with notable differences.

Inverse MixColumns :
This step is similar to the MixColumns step in encryption, but differs in the matrix used to carry out the operation.

[b0] [14 11 13 9] [c0]
| b1 | = | 9 14 11 13 | | c1 |
| b2 | | 13 9 14 11 | | c2 |
[b3] [11 13 9 14] [c3]

Inverse SubBytes :
Inverse S-box is used as a lookup table and using which the bytes are substituted during decryption.

Summary :
AES instruction set is now integrated into the CPU (offers throughput of several GB/s)to improve the speed and security of applications that use AES for encryption and

decryption. Even though its been 20 years since its introduction we have failed to break the AES algorithm as it is infeasible even with the current technology. Till date the only vulnerability remains in the implementation of the algorithm.

14. Mention the strengths and weakness of DES algorithm.

The Data Encryption Standard (DES) is a symmetric key block cipher which takes 64-bit plaintext and 56-bit key as an input and produces 64-bit cipher text as output. The DES function is made up of P and S-boxes. P-boxes transpose bits and S-boxes substitute bits to generate a cipher.

Strength- The strength of DES lies on two facts:
a. The use of 56-bit keys: 56-bit key is used in encryption, there are 256 possible keys. A brute force attack on such number of keys is impractical.
b. The nature of algorithm: Cryptanalyst can perform cryptanalysis by exploiting the characteristic of DES algorithm but no one has succeeded in finding out the weakness.

Weakness- Weakness has been found in the design of the cipher:
a. Two chosen input to an S-box can create the same output.
b. The purpose of initial and final permutation is not clear.

15. Find gcd (56, 86) using Euclid's algorithm.

Quitonent (q)	R1	R2	Remainder (r)
1	56	86	30
2	86	30	26
1	30	26	4
6	26	4	2
2	4	2	0
	2	0	

gcd is 2

16. Define Fermat Theorem.

Fermat's little theorem states that if p is a prime number, then for any integer a, the number $a^p - a$ is an integer multiple of p.

Here p is a prime number
$a^p \equiv a \pmod p$.

Special Case: If a is not divisible by p, Fermat's little theorem is equivalent to the statement that $a^{p-1}-1$ is an integer multiple of p.

$a^{p-1} \equiv 1 \pmod p$
OR
$a^{p-1} \% p = 1$
Here a is not divisible by p.

Example 1:
P = an integer Prime number

a = an integer which is not multiple of P

notes click

Let a = 2 and P = 17

According to Fermat's little theorem

$2^{17-1} \equiv 1 \bmod(17)$

we got 65536 % 17 ≡ 1

that mean (65536-1) is an multiple of 17

17. Define Euler's theorem and it's application.

notes click

Euler's theorem

Euler's theorem is a generalization of Fermat's little theorem. Euler's theorem extends Fermat's little theorem by removing the imposed condition where n must be a prime number. This allows Euler's theorem to be used on a wide range of positive integers. It states that if a random positive integer a and n are co-prime, then a raised to the power Euler's totient function $\varphi(n)$ is congruent to $1 \ (mod \, n)$. The mathematical form is as follows:

$$a^{\varphi(n)} \cong 1 \ (mod \, n)$$

However, if n is a prime number, Euler's theorem is simplified to Fermat's little theorem as follows:

$$a^{\varphi(n)} \cong 1 \ (mod \, n)$$

As $\varphi(n) = n - 1$, where n is a prime number, we can plug the value of the totient function into the equation above resulting in the equation as follows:

$$a^{n-1} \cong 1 \ (mod \, n)$$

This becomes the alternate form of Fermat's little theorem.

Application of Euler's theorem

Euler's theorem and Euler's totient function serve as a base for the modern RSA encryption algorithm. Euler's theorem is involved in the following processes of the RSA algorithm.

- Key generation process
- Encryption
- Decryption

notes click

18. How to calculate Euler's phi value of any number?

when *n* is a prime number (e.g. 2, 3, 5, 7, 11, 13), **$\varphi(n) = n-1$**.

But how about the composite numbers? You may also have noticed that, for example, 15 = 3*5 and $\varphi(15) = \varphi(3)*\varphi(5) = 2*4 = 8$. relationship is conditional:

when *m* and *n* are coprime, $\varphi(m*n) = \varphi(m)*\varphi(n)$.

The general formula to compute φ(n) is the following:

If the prime factorisation of n is given by $n = p_1^{e_1}*...*p_n^{e_n}$, then $\varphi(n) = n*(1 - 1/p_1)* ... (1 - 1/p_n)$.

For example:

- $9 = 3^2$, $\varphi(9) = 9* (1-1/3) = 6$
- $4 = 2^2$, $\varphi(4) = 4* (1-1/2) = 2$
- $15 = 3*5$, $\varphi(15) = 15* (1-1/3)*(1-1/5) = 15*(2/3)*(4/5) = 8$

19. Perform encryption and decryption using RSA Algorithm. for the following. P=7; q=11; e=17; M=8.

i. To generate key pair, given two large primes $P = 7 and Q = 11.$

ii. Calculate modulus $N = PxQ = 7x11 = 77$

$\Phi(N) = (P—l)x(Q—1) = 60.$

iii. Given $E = 17$ which is not a factor of $\Phi(N)$

iv. Select Decryption Key D:

$(DxE) mod (P-1)x(Q-1) = 1$

$D = \frac{(1+K\Phi(N))}{E} For K = 1, 2, 3, \ldots.$

$D = \frac{1+1(60)}{17} = \frac{61}{17} = 3.94 for K = 1$ Not acceptable

$D = \frac{1+2(60)}{17} = \frac{121}{17} = 7.11 for K = 2$ Not acceptable

$D = \frac{1+15(60)}{17} = \frac{901}{17} for K = 15$

$D = 53$

v. For encryption: $C = M^E mod N$

c=8^17mod77=57

vii. For decryption: $M = C^D mod N$

m=57^53mod77=8

20. Perform decryption and encryption using RSA algorithm with p=3, q=11, e=7 and M=5.

n=pxq=3x11=33
phi=2x10=20
e=7
d=(1+1x20)/7=3
c=5^7mod33=14

[notes click]

m=26^14mod33=5

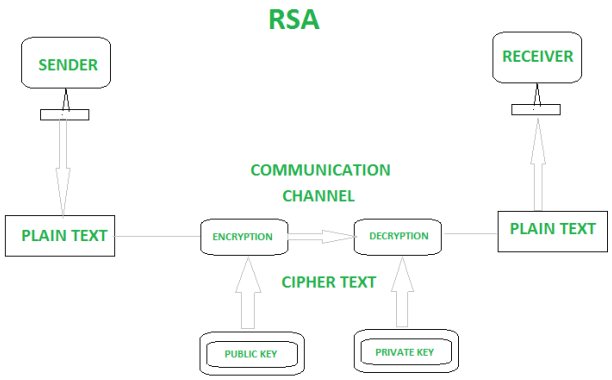
21. Discuss any two Asymmetric Technique and list their merits and demerits.

RSA stands for **Rivest, Shamir, Adleman**. These are the creators of the RSA Algorithm. It is a public-key encryption technique used for secure data transmission especially over the internet. Transmitting confidential and sensitive data over the internet through this technology is safe due to its standard encryption method. It was developed by scientist Rivest, Shamir, and Adleman at RSA Data Security Inc. in 1978. In this algorithm, a code is added to the normal message for security purposes. The algorithm is based on the factorization of large number. Large numbers cannot be easily factorized, so breaking into the message for intruders is difficult.

Working of RSA

It works on two keys:

- **Public key:** It comprises two numbers, in which one number is the result of the product of two large prime numbers. This key is provided to all the users.
- **Private key:** It is derived from the two prime numbers involved in public key and it always remains private.



Characteristics of RSA

- It is a public key encryption technique.
- It is safe for exchange of data over internet.
- It maintains confidentiality of the data.
- RSA has high toughness as breaking into the keys by interceptors is very difficult.

Advantages of RSA

notes click

- It is very easy to implement RSA algorithm.
- RSA algorithm is safe and secure for transmitting confidential data.
- Cracking RSA algorithm is very difficult as it involves complex mathematics.
- Sharing public key to users is easy.

Disadvantages of RSA

- It may fail sometimes because for complete encryption both symmetric and asymmetric encryption is required and RSA uses asymmetric encryption only.
- It has slow data transfer rate due to large numbers involved.
- It requires third party to verify the reliability of public keys sometimes.
- High processing is required at receiver's end for decryption.
- RSA can't be used for public data encryption like election voting.

Diffie-Hellman-Algorithm is primarily a protocol that is used for key exchange. Using this interactive protocol two parties will derive a common secret key by communicating each other. The security of Diffie-Hellman algorithm is mainly based on the difficulty of computing the discrete logarithms.

Applications of Diffie Hellman Algorithm:

Many protocol uses Diffie-Hellman algorithm to enhance security and few of them are:

1. Secure Shell (SSH)
2. Transport Layer Security (TLS) / Secure Sockets Layer (SSL)
3. Public Key Infrastructure (PKI)
4. Internet Key Exchange (IKE)
5. Internet Protocol Security (IPSec)

Limitations of Diffie Hellman Algorithm:

The following are the limitations of Diffie-Hellman algorithm:

1. Lack of authentication procedure.
2. Algorithm can be used only for symmetric key exchange.
3. As there is no authentication involved, it is vulnerable to man-in-the-middle attack.
4. As it is computationally intensive, it is expensive in terms of resources and CPU performance time.
5. Encryption of information cannot be performed with the help of this algorithm.
6. Digital signature cannot be signed using Diffie-Hellman algorithm.

22. User A and B exchange the key using Diffie-Hellman algorithm. Assume α=5 q=11 XA=2 XB=3.
    Find the value of YA, YB and k.

notes click

$Y_A = á^{XA} \bmod q = 5^2 \bmod 11 = 3$

$Y_B = á^{XB} \bmod q = 5^3 \bmod 11 = 4$

$K_A = Y_B^{XA} \bmod q = 4^2 \bmod 11 = 5$

$K_B = Y_A^{XB} \bmod q = 33 \bmod 11 = 5$

23. What is MAC.

Short for **Media Access Control**, or **MAC address**. Known as a **physical address** and **hardware address** whose number is uniquely formatted in hexadecimal format and given to each computer or network device on a computer network.

MAC addresses can be 48-bit or 64-bit numbers divided into two parts. A unique three-byte **OUI** (**Organizationally Unique Identifier**) identifies the device's manufacturer and must be purchased from the IEEE. The manufacturer assigns the remaining three or five bytes. After the number is generated, it's considered burned into the firmware of the network access hardware.

Because a MAC address is a unique address, devices on a network do not share the same MAC address.

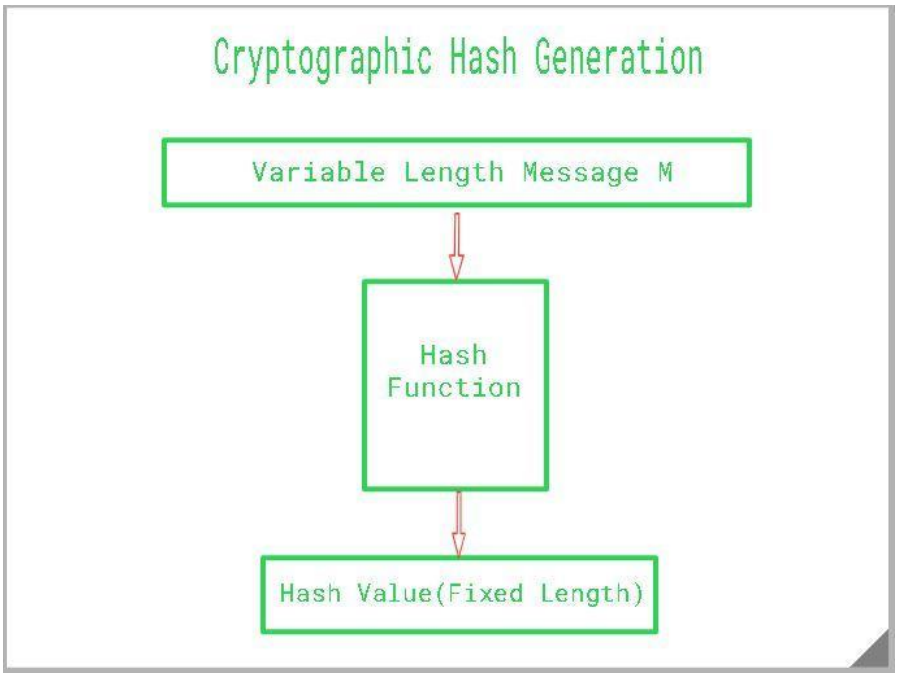
Example of a MAC address

D4-BE-D9-8D-46-9A

24. What is Hash Function

Cryptographic Hash is a Hash function that takes random size input and yields a fixed-size output. It is easy to calculate but challenging to retrieve original data. It is strong and difficult to duplicate the same hash with unique inputs and is a one-way function so revert is not possible. Hashing is also known by different names such as Digest, Message Digest, Checksum, etc.

[notes click]



Properties Of Cryptography Hash Function

The ideal cryptographic hash function has the following main properties:

1. **Deterministic:** This means that the same message always results in the same hash.
2. **Quick:** It is quick to compute the hash value for any given message.
3. **Avalanche Effect:** This means that every minor change in the message results in a major change in the hash value.
4. **One-Way Function:** You cannot reverse the cryptographic hash function to get to the data.
5. **Collision Resistance:** It is infeasible to find two different messages that produce the same hash value.

25. Define SHA-1

SHA-1 or Secure Hash Algorithm 1 is a cryptographic hash function which takes an input and produces a 160-bit (20-byte) hash value. This hash value is known as a message digest. This message digest is usually then rendered as a hexadecimal number which is 40 digits long. It is a U.S. Federal Information Processing Standard and was designed by the United States National Security Agency. SHA-1 is now considered insecure since 2005. Major tech giants browsers like Microsoft, Google, Apple and Mozilla have stopped accepting SHA-1 SSL certificates by 2017. To calculate cryptographic hashing value in Java, **MessageDigest Class** is used, under the package **java.security**. MessageDigest Class provides following cryptographic hash function to find hash value of a text as follows:

- MD2
- MD5
- SHA-1
- SHA-224
- SHA-256
- SHA-384
- SHA-512

[notes click]

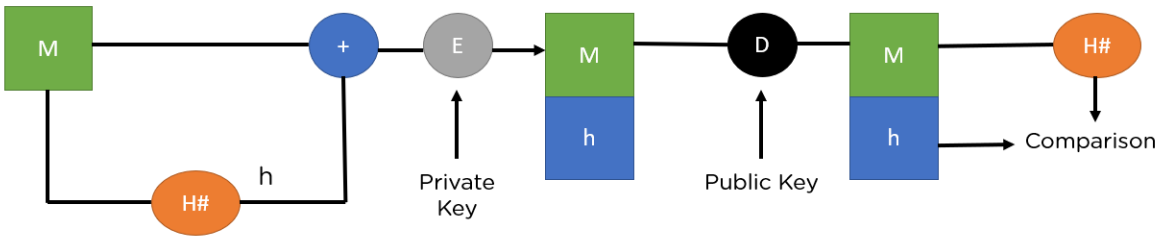
These algorithms are initialized in static method called **getInstance()**. After selecting the algorithm the message digest value is calculated and the results are returned as a byte array. BigInteger class is used, to convert the resultant byte array into its signum representation. This representation is then converted into a hexadecimal format to get the expected MessageDigest. **Examples:**

***Input** : hello world **Output** : 2aae6c35c94fcfb415dbe95f408b9ce91ee846ed **Input** : GeeksForGeeks **Output** : addf120b430021c36c232c99ef8d926aea2acd6b*

26. Write and explain the digital signature algorithm.

The objective of digital signatures is to authenticate and verify documents and data. This is necessary to avoid tampering and digital modification or forgery during the transmission of official documents.

With one exception, they work on the public key cryptography architecture. Typically, an asymmetric key system encrypts using a public key and decrypts with a private key. For digital signatures, however, the reverse is true. The signature is encrypted using the private key and decrypted with the public key. Because the keys are linked, decoding it with the public key verifies that the proper private key was used to sign the document, thereby verifying the signature's provenance.



M - Plaintext

H - Hash function

h - Hash digest

'+' - Bundle both plaintext and digest

E - Encryption

D - Decryption

The image above shows the entire process, from the signing of the key to its verification. So, go through each step to understand the procedure thoroughly.

notes click

- Step 1: M, the original message is first passed to a hash function denoted by H# to create a digest.
- Step 2: Next, it bundles the message together with the hash digest h and encrypts it using the sender's private key.
- Step 3: It sends the encrypted bundle to the receiver, who can decrypt it using the sender's public key.
- Step 4: Once it decrypts the message, it is passed through the same hash function (H#), to generate a similar digest.
- Step 5: It compares the newly generated hash with the bundled hash value received along with the message. If they match, it verifies data integrity.

There are two industry-standard ways to implement the above methodology. They are:

1. RSA Algorithm
2. DSA Algorithm

27. What are the properties a digital signature should have?
    - must depend on the message signed
    - must use information unique to sender
    - to prevent both forgery and denial
    - must be relatively easy to produce
    - must be relatively easy to recognize & verify
    - be computationally infeasible to forge
    - with new message for existing digital signature
    - with fraudulent digital signature for given message
    - be practical save digital signature in storage

- Properties of Digital Signatures
    - Unforgeable
    - Authentic
    - Can't be modified once sent
    - Not reusable
    - Prevent repudiation

28. What are the characteristics of good Password?
    - At least 12 characters (required for your Muhlenberg password)—the more characters, the better.
    - A mixture of both uppercase and lowercase letters.

notes click

- A mixture of letters and numbers.
- Inclusion of at least one special character, e.g., ! @ # ?]

29. What IP security?

The **IP security (IPSec)** is an Internet Engineering Task Force (IETF) standard suite of protocols between 2 communication points across the IP network that provide data authentication, integrity, and confidentiality. It also defines the encrypted, decrypted and authenticated packets. The protocols needed for secure key exchange and key management are defined in it.

Uses of IP Security –

IPsec can be used to do the following things:

- To encrypt application layer data.
- To provide security for routers sending routing data across the public internet.
- To provide authentication without encryption, like to authenticate that the data originates from a known sender.
- To protect network data by setting up circuits using IPsec tunneling in which all data is being sent between the two endpoints is encrypted, as with a Virtual Private Network(VPN) connection

Components of IP Security –

It has the following components:

1. **Encapsulating Security Payload (ESP) –**
   It provides data integrity, encryption, authentication and anti replay. It also provides authentication for payload.
2. **Authentication Header (AH) –**
   It also provides data integrity, authentication and anti replay and it does not provide encryption. The anti replay protection, protects against unauthorized transmission of packets. It does not protect data's confidentiality.

Internet Key Exchange (IKE) –

It is a network security protocol designed to dynamically exchange encryption keys and find a way over Security Association (SA) between 2 devices.

30. What is Web security?

In general, web security refers to the protective measures and protocols that organizations adopt to protect the organization from cyber criminals and threats that use the web channel. Web security is critical to business continuity and to protecting data, users and companies from risk.

What are the Benefits of Web Security?

For a modern enterprise, effective web security has broad technical and human benefits:

- **Protect your business and stay compliant** by preventing loss of sensitive data
- **Protect customers and employees** by securing their private information
- **Avoid costly service interruptions** by preventing infections and exploits
- **Offer a better user experience** by helping your users stay safe and productive
- **Maintain customer loyalty and trust** by staying secure and out of the news

notes click

What Does Web Security Protect Against?
Web security casts a wide net to protect users and endpoints from malicious emails, encrypted threats, malicious or compromised websites and databases, malicious redirects, hijacking, and more. Let's look at a few of the most common threats in more detail:

- **Ransomware:** These attacks encrypt data, and then demand a ransom payment in exchange for a decryption key. In a double-extortion attack, your data is also exfiltrated.
- **General malware:** Countless variants of malware exist that can lead to anything from data leaks, spying, and unauthorized access to lockouts, errors, and system crashes.
- **Phishing:** Often carried out through email, text messages, or malicious websites, these attacks trick users into things like divulging login credentials or downloading spyware.
- **SQL injection:** These attacks exploit an input vulnerability in a database server, allowing an attacker to execute commands that let them retrieve, manipulate, or delete data.
- **Denial of service (DoS):** These attacks slow or even shut down a network device such as a server by sending it more data than it can process. In distributed DoS—that is, a DDoS attack—this is carried out by many hijacked devices at once.
- **Cross-site scripting (XSS):** In this type of injection attack, an attacker introduces malicious code to a trusted website by entering it in an unprotected user input field.

31. What is Firewall?

A firewall is a network security device that monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic based on a defined set of security rules.

Firewalls have been a first line of defense in network security for over 25 years. They establish a barrier between secured and controlled internal networks that can be trusted and untrusted outside networks, such as the Internet.

A firewall can be hardware, software, or both.

Types of Firewalls

- **Packet filtering**

  A small amount of data is analyzed and distributed according to the filter's standards.

[notes click]

- **Proxy service**

  Network security system that protects while filtering messages at the application layer.

- **Stateful inspection**

  Dynamic packet filtering that monitors active connections to determine which network packets to allow through the Firewall.

- **Next Generation Firewall (NGFW)**

  Deep packet inspection Firewall with application-level inspection

What Firewalls Do?

A Firewall is a necessary part of any security architecture and takes the guesswork out of host level protections and entrusts them to your network security device. Firewalls, and especially Next Generation Firewalls, focus on blocking malware and application-layer attacks, along with an integrated intrusion prevention system (IPS), these Next Generation Firewalls can react quickly and seamlessly to detect and react to outside attacks across the whole network. They can set policies to better defend your network and carry out quick assessments to detect invasive or suspicious activity, like malware, and shut it down.

32. What are the function areas of IP security?

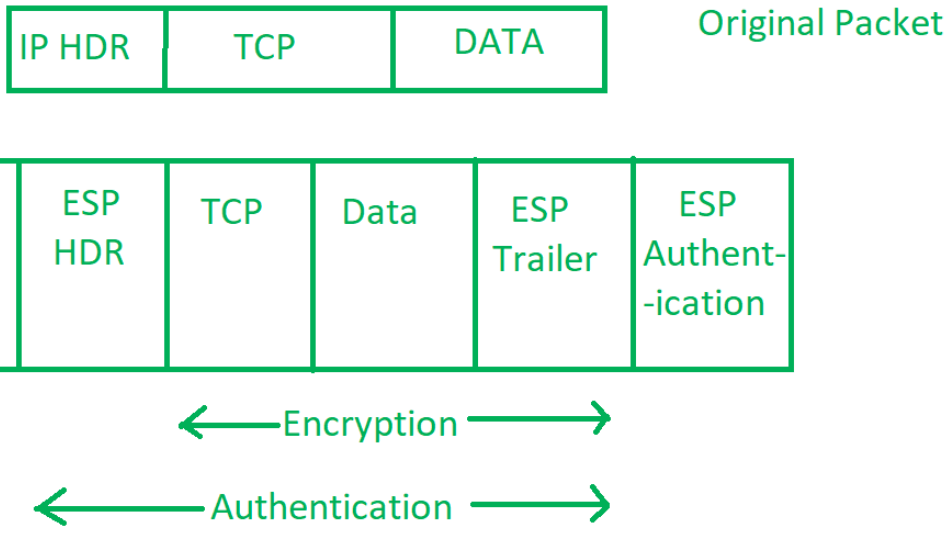
Components of IP Security –

It has the following components:

1. **Encapsulating Security Payload (ESP) –**
   It provides data integrity, encryption, authentication and anti replay. It also provides authentication for payload.
2. **Authentication Header (AH) –**
   It also provides data integrity, authentication and anti replay and it does not provide encryption. The anti replay protection, protects against unauthorized transmission of packets. It does not protect data's confidentiality.

[notes click]

3. **Internet Key Exchange (IKE) –**
   It is a network security protocol designed to dynamically exchange encryption keys and find a way over Security Association (SA) between 2 devices. The Security Association (SA) establishes shared security attributes between 2 network entities to support secure communication. The Key Management Protocol (ISAKMP) and Internet Security Association which provides a framework for authentication and key exchange. ISAKMP tells how the set up of the Security Associations (SAs) and how direct connections between two hosts that are using IPsec.
   Internet Key Exchange (IKE) provides message content protection and also an open frame for implementing standard algorithms such as SHA and MD5. The algorithm's IP sec users produces a unique identifier for each packet. This identifier then allows a device to determine whether a packet has been correct or not. Packets which are not authorized are discarded and not given to receiver.



33. What are the positive and negative effects of firewall?

Advantages of Firewall

- A Firewall prevents hackers and remote access.
- It protects data.
- It ensures better privacy and security.
- It protects from Trojans.

notes click

- A network-based Firewall, like a router, can offer protection to multiple systems, while an OS-based Firewall can protect individual systems.

Disadvantages of Firewall

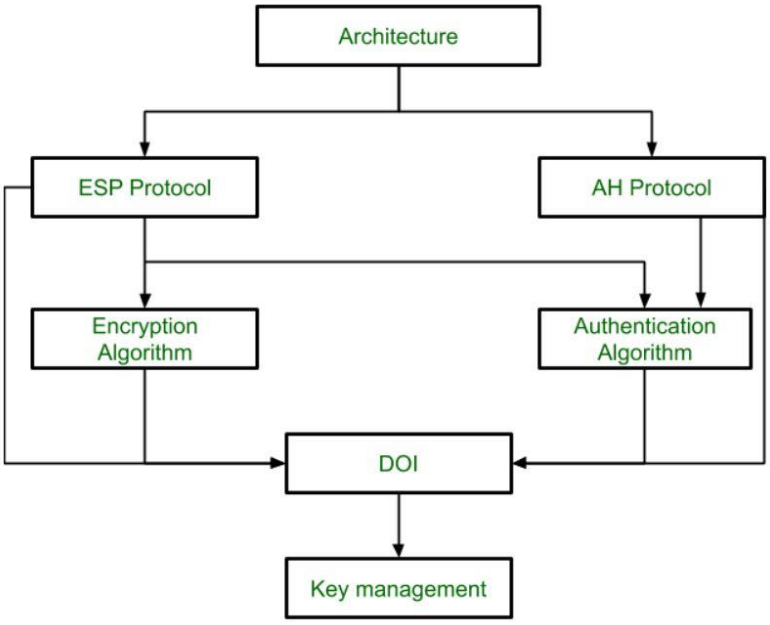
- **Cost:** Installation of a Firewall can be costly depending on the sophistication required.
- **Performance:** This is affected as each packet has to be verified for authenticity before it is allowed into the network.
- **Virus and Malware:** There are a few limitations in a Firewall like its inability to prevent virus and malware attacks for which separate applications would be required, at the individual system level.
- A network-level Firewall might bring in a false sense of security in employees and make them slacken on securing individual systems. Companies need to make all employees understand the concept of a Firewall and the importance of a Firewall for information security and their responsibility.
- Firewall maintenance and up-gradation require extra manpower and resources.

34. Explain the architecture of IP Security

IPSec (IP Security) architecture uses two protocols to secure the traffic or data flow. These protocols are ESP (Encapsulation Security Payload) and AH (Authentication Header). IPSec Architecture includes protocols, algorithms, DOI, and Key Management. All these components are very important in order to provide the three main services:

- Confidentiality
- Authentication
- Integrity

IP Security Architecture:



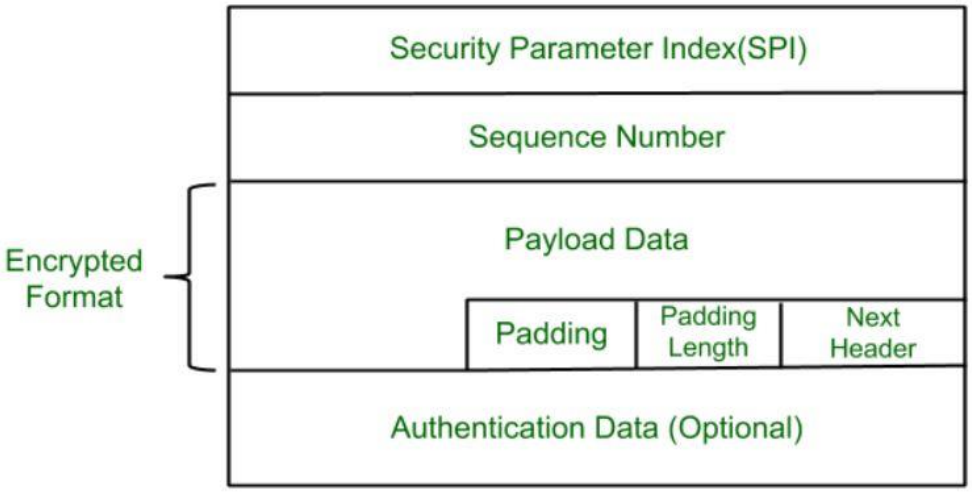
1. Architecture: Architecture or IP Security Architecture covers the general concepts, definitions, protocols, algorithms, and security requirements of IP Security technology.
2. ESP Protocol: ESP(Encapsulation Security Payload) provides a confidentiality service. Encapsulation Security Payload is implemented in either two ways:

- ESP with optional Authentication.

[notes click]

- ESP with Authentication.

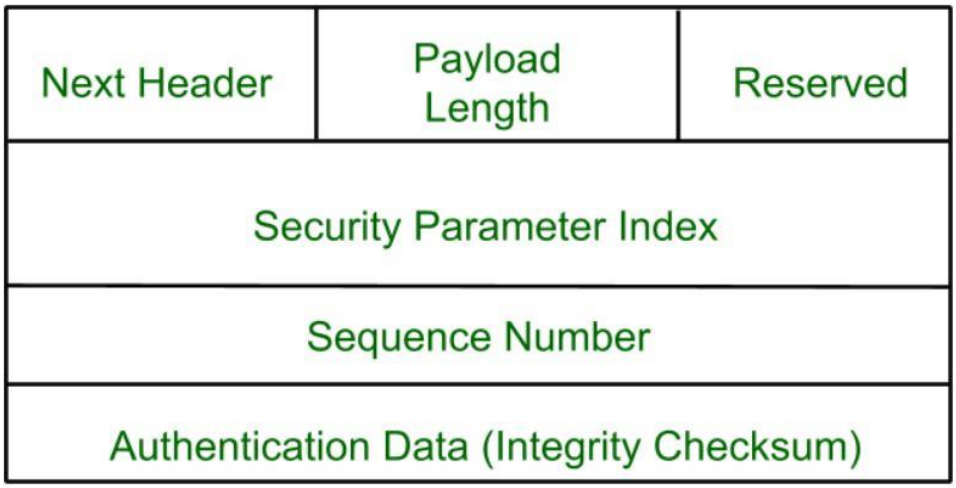
Packet Format:



- **Security Parameter Index(SPI):** This parameter is used by Security Association. It is used to give a unique number to the connection built between the Client and Server.
- **Sequence Number:** Unique Sequence numbers are allotted to every packet so that on the receiver side packets can be arranged properly.
- **Payload Data:** Payload data means the actual data or the actual message. The Payload data is in an encrypted format to achieve confidentiality.
- **Padding:** Extra bits of space are added to the original message in order to ensure confidentiality. Padding length is the size of the added bits of space in the original message.
- **Next Header:** Next header means the next payload or next actual data.
- **Authentication Data** This field is optional in ESP protocol packet format.

3. Encryption algorithm: The encryption algorithm is the document that describes various encryption algorithms used for Encapsulation Security Payload.

4. AH Protocol: AH (Authentication Header) Protocol provides both Authentication and Integrity service. Authentication Header is implemented in one way only: Authentication along with Integrity.



Authentication Header covers the packet format and general issues related to the use of AH for packet authentication and integrity.

notes click

5. Authentication Algorithm: The authentication Algorithm contains the set of documents that describe the authentication algorithm used for AH and for the authentication option of ESP.
6. DOI (Domain of Interpretation): DOI is the identifier that supports both AH and ESP protocols. It contains values needed for documentation related to each other.
7. Key Management: Key Management contains the document that describes how the keys are exchanged between sender and receiver.

35. What you understand by Malicious Software. How it's harm to computer

Malware is a software that gets into the system without user consent with an intention to steal private and confidential data of the user that includes bank details and password. They also generates annoying pop up ads and makes changes in system settings

They get into the system through various means:

1. Along with free downloads.
2. Clicking on suspicious link.
3. Opening mails from malicious source.
4. Visiting malicious websites.
5. Not installing an updated version of antivirus in the system.

Types:

1. Virus
2. Worm
3. Logic Bomb
4. Trojan/Backdoor
5. Rootkit
6. Advanced Persistent Threat
7. Spyware and Adware

What is computer virus:

Computer virus refers to a program which damages computer systems and/or destroys or erases data files

- Letter looks like they are falling to the bottom of the screen.
- The computer system becomes slow.
- The size of available free memory reduces.
- The hard disk runs out of space.
- The computer does not boot.

Worm:

A worm is a destructive program that fills a computer system with self-replicating information, clogging the system so that its operations are slowed down or stopped.

Trojan / Backdoor:

Trojan Horse is a destructive program. It usually pretends as computer games or application software. If executed, the computer system will be damaged.

Spyware and Adware:

Normally gets installed along with free software downloads. Spies on the end-user, attempts to redirect the user to specific sites. Main tasks: Behavioral surveillance and advertising with pop up ads Slows down the system.

notes click

36. List and Brief, the different generation of antivirus software

First Generation

Simple scanners involve a record of program length. This generation can identify a virus only if it has a virus signature. These scanners are signature specific, so if any kind of virus attacks the system, this antivirus fails.

Second Generation

Heuristic scanners that conduct integrity checking with checksums. This generation of antivirus identifies code blocks linked to virus attacks.

Third Generation

Activity traps, which employ memory resident, detect infected actions. This generation consists of memory-resident antivirus software that detects and halts the working virus patterns.

Fourth Generation

Full-featured protection, a suite of antivirus techniques, and access control capability. This generation is known as behavior-blocking software, which offers features like scanning and monitoring. This antivirus works alongside the operating system and detects activities that match virus-like patterns. Any uncertainty is identified. This generation emphasizes attack prevention rather than virus detection.

37. Explain the security with antivirus software.

Antivirus software is a program or set of programs that are designed to prevent, search for, detect, and remove software viruses, and other malicious software like worms, trojans, adware, and more.

Why Do I Need Antivirus Software?

These antivirus tools are critical for users to have installed and up-to-date because a computer without antivirus software protection will be infected within minutes of connecting to the internet. The bombardment is constant, which means antivirus companies have to update their detection tools regularly to deal with the more than 60,000 new pieces of malware created daily.

Today's malware (an umbrella term that encompasses computer viruses) changes appearance quickly to avoid detection by older, definition-based antivirus software. Viruses can be programmed to cause damage to your device, prevent a user from accessing data, or to take control of your computer.

notes click

What Does AntiVirus Software Do?

Several different companies build antivirus software and what each offer can vary but all perform some essential functions:

- Scan specific files or directories for any malware or known malicious patterns
- Allow you to schedule scans to automatically run for you
- Allow you to initiate a scan of a particular file or your entire computer, or of a CD or flash drive at any time.
- Remove any malicious code detected –sometimes you will be notified of an infection and asked if you want to clean the file, other programs will automatically do this behind the scenes.
- Show you the 'health' of your computer

Always be sure you have the best, up-to-date security software installed to protect your computers, laptops, tablets, and smartphones.

What Are the Benefits of Antivirus Software?

Antivirus solutions protect more than just laptops, office computers, smartphones and tablets. They protect precious memories, music and photo libraries, and important documents from destruction by malware. Make sure your protection is up to the challenge of defending against the latest threats.

Modern antivirus solutions are capable of:

- Detecting, blocking, and removing viruses, malware, and ransomware
- Preventing identity theft and block phishing and fraud
- Warning about dangerous websites and links before you click
- Scanning the Dark Web to find if an email address has been compromised
- Keeping online accounts protected with secure password encryption
- Providing simple training to teach you and your family how to be even safer online
- Tuning up your computer to keep it running smoothly, just like new

How Does Antivirus Software Work?

Many antivirus software programs still download malware definitions straight to your device and scan your files in search of matches. But since, as we mentioned, most malware regularly morphs in appearance to avoid detection, Webroot works differently. Instead of storing examples of recognized malware on your device, it stores malware definitions in the cloud. This allows us to take up less space, scan faster, and maintain a more robust threat library.