What is computer security & explain.

- Computer security basically is the protection of computer systems and information from harm, theft, and unauthorized use. It is the process of preventing and detecting unauthorized use of our computer system.
- Computer security ensures the confidentiality, integrity, and availability of computers and their stored data.

Types of Attacks :

Denial of service (DDoS):

- This is an attack used to restrict the user's access to the system resources by flooding the server with useless traffic.

Malware attack:

- A malware attack involves the deployment of malicious software, commonly known as malware, with the intent to compromise the security, or data of a computer system or network.

Man in the middle :

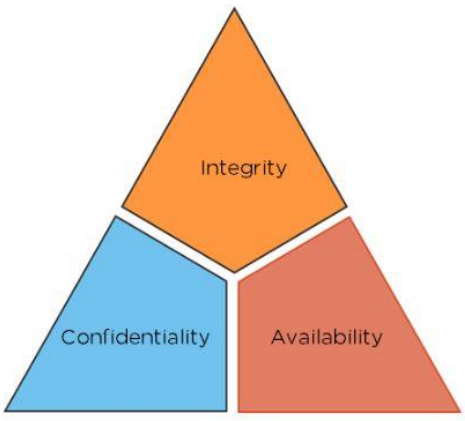
- A Man-in-the-Middle (MitM) attack is a type of cyberattack where an attacker intercepts communication between two parties without their knowledge in order to capture sensitive information,

Phishing:

- Phishing is a type of cyberattack that involves the use of fraudulent emails, messages, or websites to deceive individuals into revealing sensitive information, such as usernames, passwords

The CIA Triad :

- Computer security is mainly concerned with three main areas:
    1. **Confidentiality.**
    2. **Integrity**
    3. **Availability**



Confidentiality :

- Confidentiality involves protecting sensitive data private and safe from unauthorized access.
- This includes protecting information from bad actors with malicious intent, as well as limiting access to only authorized individuals within an organization.
- Different levels of protection can be applied based on the sensitivity of the data.
- Example: military secrets and their communication.

Integrity :

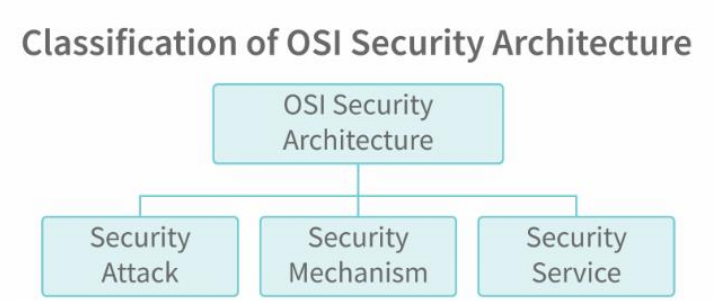
- The principles of integrity assert that information and functions can be added, altered, or removed only by authorized people and means.
- Maintaining data integrity is important to make sure data and business analysts are accessing accurate information.
- Data shown to the public must also maintain integrity so that customers can trust the organization.
- Example: incorrect data entered by a user in the database.

Availability:

- Availability guarantees that authorized individuals can consistently access information and resources when needed.
- Systems, applications, and data will lose their value if they are not accessible by their authorized users whenever they require them.
- Availability can be compromised if there is a hardware or software failure, natural disasters, power failure, or human error.
- Example : If a website is consistently available, customers can access it whenever they want to shop. This enhances their satisfaction and encourages repeat visits.

Explain OSI security architecture model.

- The security model is designed to provide security to organizations to prevent their data from being breached.
- The OSI security architecture is useful to managers as a way of organizing the task of providing security.
- The OSI security architecture focuses on the following components :

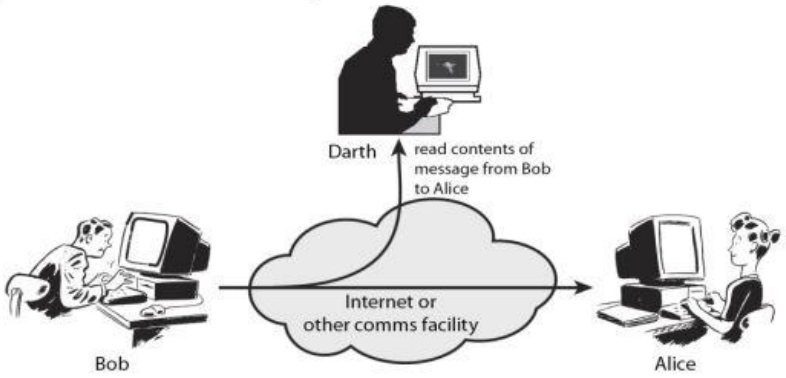


Security attack :

- An attack is any attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an asset
- A security attack means any action that puts the data or overall security of the system of an individual organisation at risk.
- There are majorly 2 types of attacks ,
  - Passive attacks
  - Active attacks.

Passive attacks –

- A passive attack is a kind of attack in which the data that is sent from the sender to the receiver is read by the attacker in the middle of the transmission.
- In this type of attack the attacker does not modify or corrupt the data and does not affect system resources.



There passive attack is classified into two types – a) Release of message contents , b) Traffic analysis.

Active attacks –

- Active attacks involve some modification of the data stream or the creation of a false stream.
- It is subdivided into four categories **: masquerade, replay, modification of messages, and denial of service.**
- A **masquerade** takes place when one entity pretends to be a different entity.
- **Replay** involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect.
- **Modification of messages** simply means that some portion of a legitimate message is altered, or that messages are delayed or reordered, to produce an unauthorized effect.
- The **denial of service prevents** or inhibits the normal use or management of communications facilities.

- **Security mechanism** : A security mechanism is a means to provide a sevice. These mechanisms are designed to enhance the security of data and communications.

Specific Security Mechanisms:

- Specific security mechanisms are techniques and methods that are employed to enhance the security of data and communications in a network environment.
- Some common specific security mechanisms include:
    - Encipherment
    - Digital Signature mechanisms
    - Access Control
    - Data Integrity
    - Authentication Exchange
    - Traffic Padding
    - Routing Control
    - Notarization

Pervasive Security Mechanisms

- The Mechanisms that is not specific to any particular OSI security service or protocol layer is known as Pervasive Security Mechanisms.

- Some common Pervasive Security Mechanisms include :
  - Trusted Functionality
  - Security Label
  - Event Detection
  - Security Audit Trail
  - Security Recovery

Security services :

- A security service is “A processing or communication service that is provided by a system to give a specific kind of protection to system resources”.
- The OSI security architecture classifies security services as follows:

- Authentication:
  - Peer entity authentication
  - *Data origin authentication*
- Access Control Service
- Data Confidentiality:
  - Connection confidentiality
  - Connectionless confidentiality
  - Selective field confidentiality
  - Traffic flow confidentiality
- Data integrity
  - Connection integrity with recovery
  - Connection integrity without recovery
  - Selective field connection integrity
  - Connectionless integrity
  - Selective field connectionless integrity
- Non-repudiation
  - Non-repudiation with proof of origin
  - Non-repudiation with proof of delivery

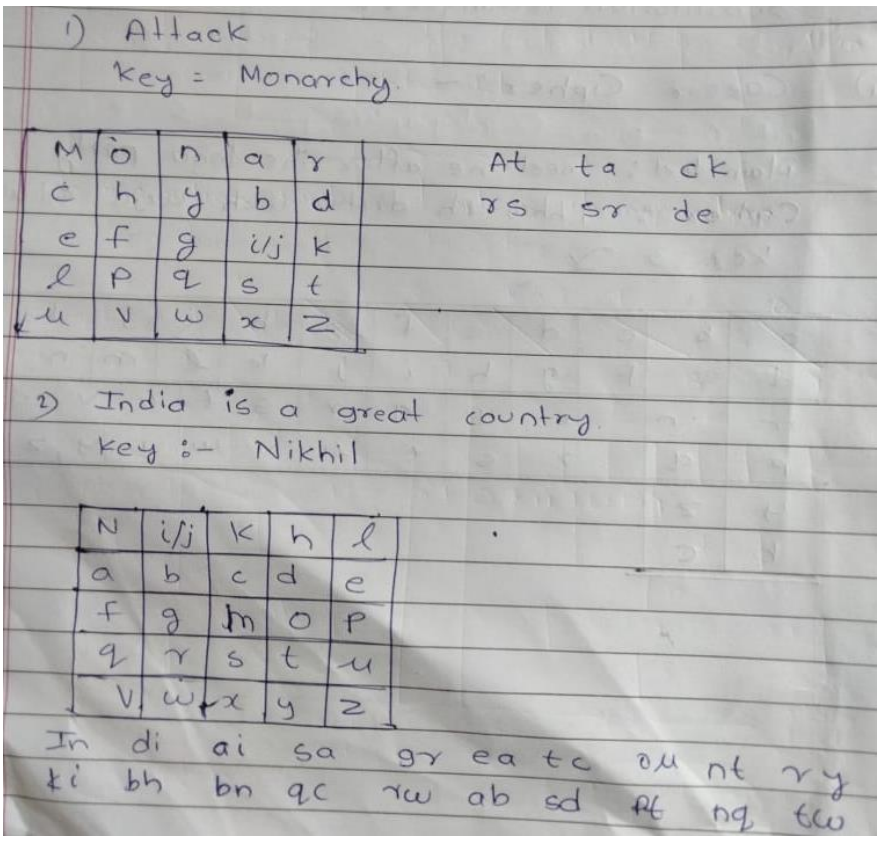
Any example on substitution & transportation techniques

- In substitution Cipher Technique, plain text characters are replaced with other characters, numbers and symbols.
- Involves replacing plaintext letters or groups of letters with ciphertext letters or groups of letters according to a specific algorithm or key.
- The example of substitution Cipher is Caesar Cipher, monoalphabetic cipher, and polyalphabetic cipher,playfair cipher.

Example of playfair cipher –

Rules –

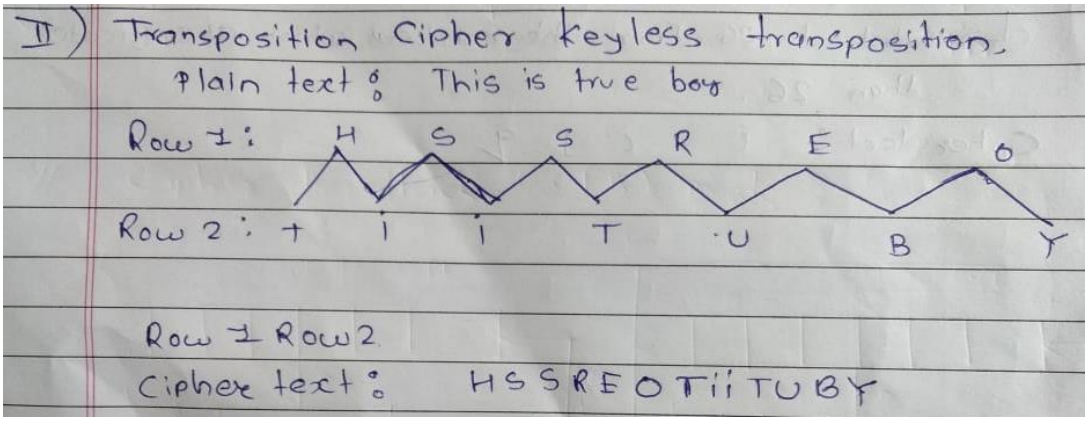
- Create a 5*5 matrix.
- The plaintext is split into pairs of two letters (digraphs). If there is an odd number of letters, a Z is added to the last letter.
- **If both the letters are in the same column**: Take the letter below each one
- **If both the letters are in the same row**: Take the letter to the right of each one.
- Form a rectangle with the two letters and take the letters on the horizontal opposite corner of the rectangle.



- In transposition Cipher Technique, plain text characters are rearranged with respect to the position.
- Transposition Cipher's forms are: Key-less transposition cipher and keyed transposition cipher.
- While in transposition Cipher Technique, The position of the character is changed but character's identity is not changed.

Key-less transposition cipher :

First write it on two lines in a zig-zag pattern (or rail fence). The cipher text is produced by transcribing the first row followed by the second row.



Encrypt: **NOTHING IS AS IT SEEMS**

N T I G S S T E M
O H N I A I S E S

Cipher text: **NTIGS STEMO HNIAI SES**

- To decrypt, write half the letters on one line, half on the second.

Explain columnar transportation technique in detail?

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

Encryption :

- The message is written out in rows of a fixed length, and then read out again column by column, and the columns are chosen in some scrambled order.
- We first pick a keyword for our encryption.
- As an example, encrypt the message "The tomato is a plant in the nightshade family" using the keyword *tomato*. We get the grid given below.

T	O	M	A	T	O
5	3	2	1	6	4
T	H	E	T	O	M
A	T	O	I	S	A
P	L	A	N	T	I
N	T	H	E	N	I
G	H	T	S	H	A
D	E	F	A	M	I
L	Y	X	X	X	X

- By using the sequence of numbers of the keyword TOMATO , i.e 123456 The final ciphertext is thus "TINES AXEOA HTFXH TLTHE YMAII AIXTA PNGDL OSTNH MX".

Decryption :

- As an example, we shall decrypt the ciphertext "ARESA SXOST HEYLO IIAIE XPENG DLLTA HTFAX TENHM WX" given the keyword *potato*.
- We start by writing out the keyword and the order of the letters. There are 42 letters in the ciphertext, and the keyword has six letters, so we need 42 ÷ 6 = 7 rows.

P	O	T	A	T	O
4	2	5	1	6	3

- Now we start by filling in the columns in the order given by the alphabetical order of the keyword, starting with the column headed by "A". After the first column is entered we have the grid shown to the right.
- We continue to add columns in the order specified by the keyword.

P	O	T	A	T	O
4	2	5	1	6	3
	O		A		
	S		R		
	T		E		
	H		S		
	E		A		
	Y		S		
	L		X		

After inserting the second column.

P	O	T	A	T	O
4	2	5	1	6	3
	O		A		O
	S		R		I
	T		E		I
	H		S		A
	E		A		I
	Y		S		E
	L		X		X

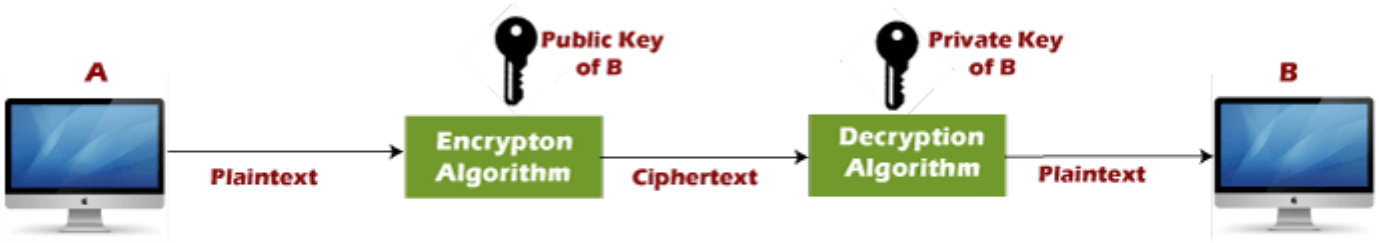
After inserting the third column.

P	O	T	A	T	O
4	2	5	1	6	3
P	O	T	A	T	O
E	S	A	R	E	I
N	T	H	E	N	I
G	H	T	S	H	A
D	E	F	A	M	I
L	Y	A	S	W	E
L	L	X	X	X	X

The completely reconstructed grid.

Explain RSA algorithm in detail?

- RSA algorithm is an asymmetric cryptography algorithm. Asymmetric actually means that it works on two different keys i.e. Public Key and Private Key.
- **P**ublic Key is given to everyone and the Private key is kept private**.**
  The Public key is used for encryption, and the Private Key is used for decryption.
- The two keys are linked, but the private key cannot be derived from the public key. The public key is well known, but the private key is secret and it is known only to the user who owns the key.
- It means that everybody can send a message to the user using user's public key. But only the user can decrypt the message using his private key.



Encryption/decryption using public/private keys

RSA algorithm uses the following procedure to generate public and private keys:

This example shows how we can encrypt plaintext 9 using the RSA public-key encryption algorithm. This example uses prime numbers 7 and 11 to generate the public and private keys.

Explanation:

Step 1: Select two large prime numbers, p, and **q**.

p = 7

q = 11

Step 2: Multiply these numbers to find **n = p x q,** where **n** is called the modulus for encryption and decryption.

First, we calculate

n = p x q

n = 7 x 11

n = 77

Step 3: Choose a number **e** less that **n**, such that n is relatively prime to **(p - 1) x (q -1).** It means that **e** and **(p - 1) x (q - 1)** have no common factor except 1. Choose "e" such that 1<e < ϕ (n), e is prime to ϕ (n), gcd (e, d (n)) =1.

Second, we calculate

ϕ (n) = (p - 1) x (q-1)

ϕ (n) = (7 - 1) x (11 - 1)

ϕ (n) = 6 x 10

ϕ (n) = 60

Let us now choose relative prime e of 60 as 7.

Thus the public key is <e, n> = (7, 77)

Step 4: A plaintext message **m** is encrypted using public key <e, n>. To find ciphertext from the plain text following formula is used to get ciphertext C.

To find ciphertext from the plain text following formula is used to get ciphertext C.

$C = m^e \bmod n$

$C = 9^7 \bmod 77$

C = 37

Step 5: The private key is <d, n>. To determine the private key, we use the following formula d such that:

$D_e \bmod \{(p - 1) x (q - 1)\} = 1$

7d mod 60 = 1, which gives d = 43

The private key is <d, n> = (43, 77)

Step 6: A ciphertext message **c** is decrypted using private key <d, n>. To calculate plain text **m** from the ciphertext c following formula is used to get plain text m.

$m = c^d \bmod n$

$m = 37^{43} \bmod 77$

m = 9

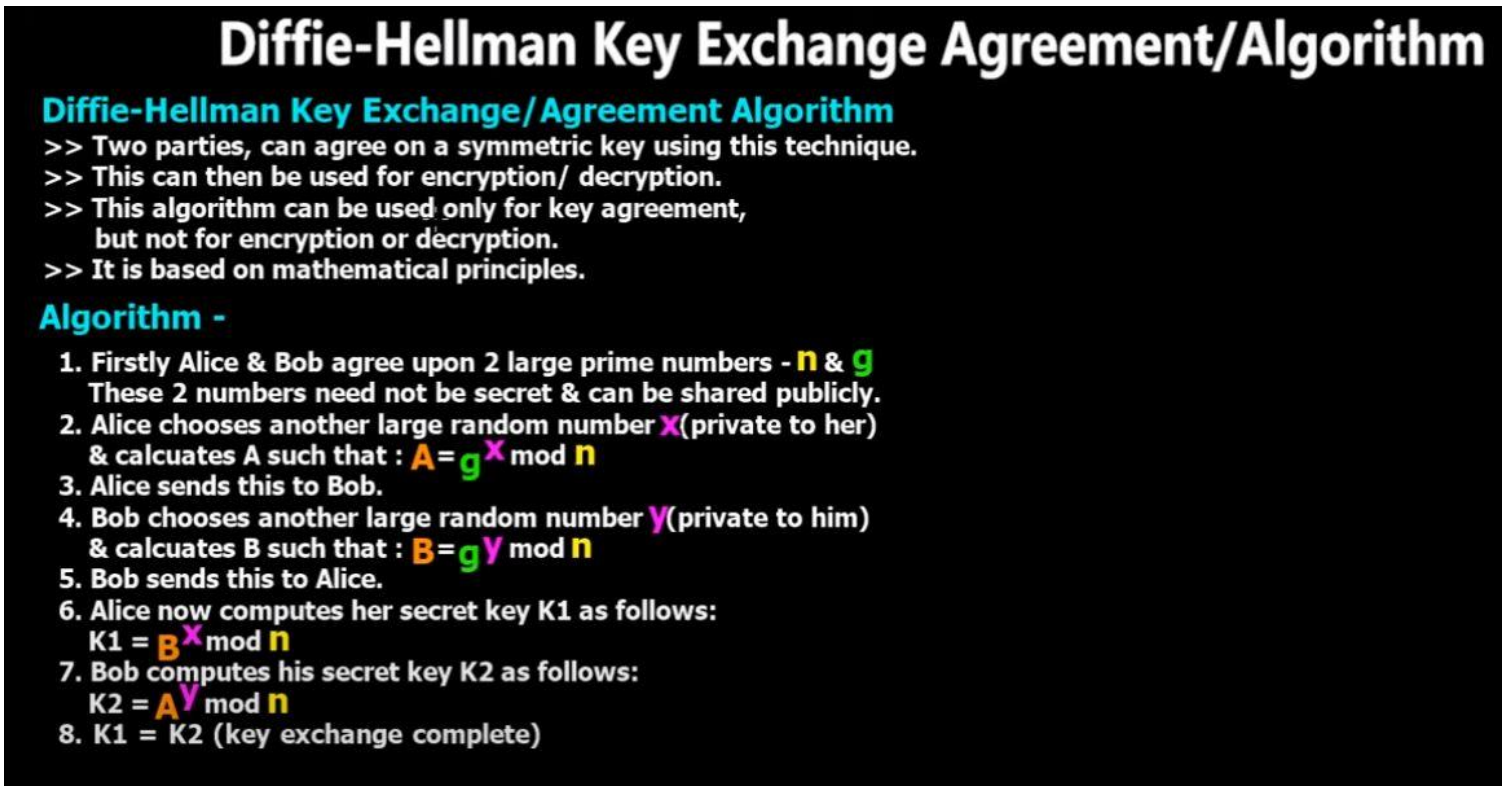
In this example, Plain text = 9 and the ciphertext = 37

Difference between symmetric & asymmetric cipher

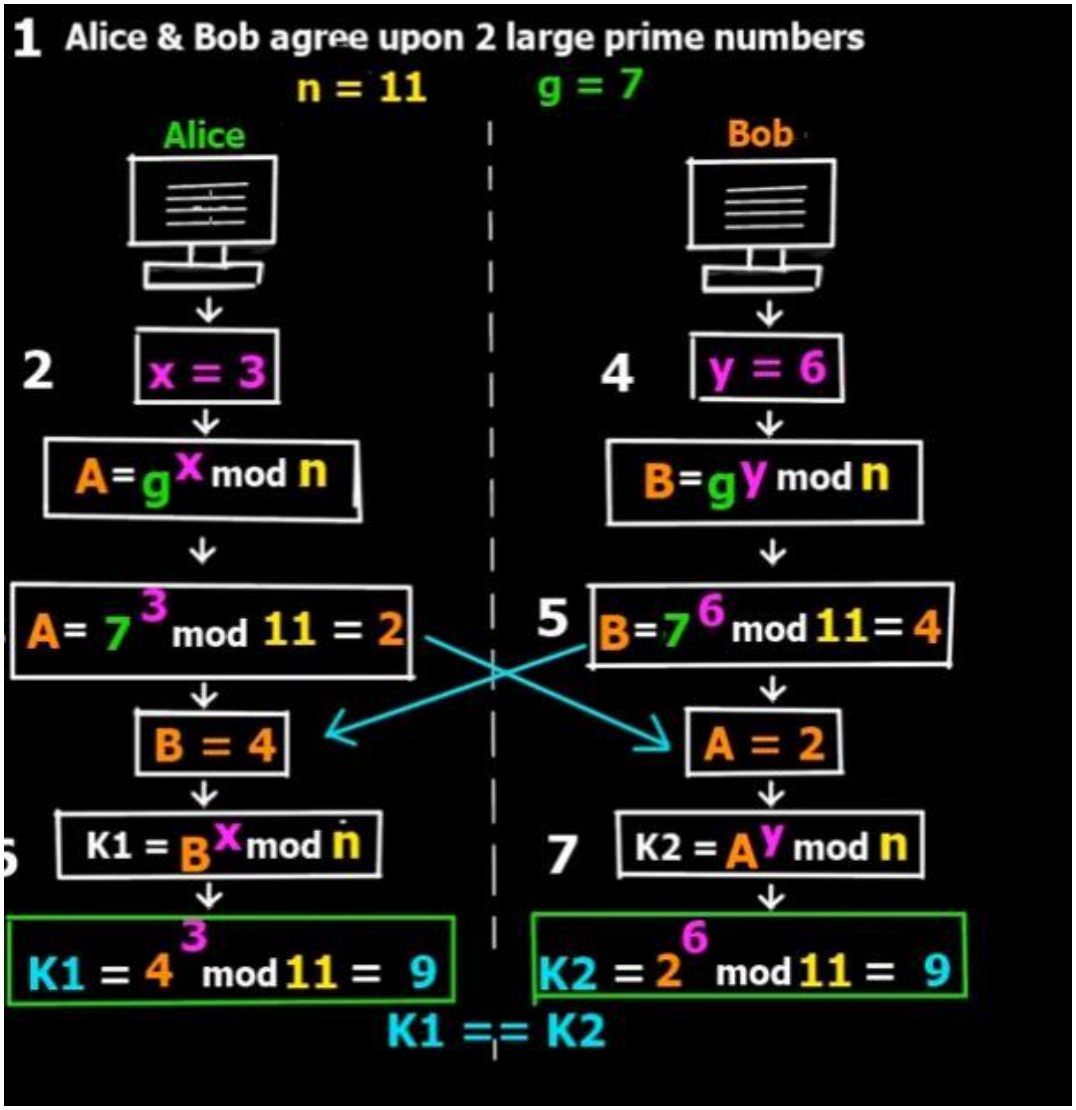
Symmetric Key Encryption	Asymmetric Key Encryption
It only requires a single key for both encryption and decryption.	It requires two keys, a public key and a private key, one to encrypt and the other one to decrypt.
The size of cipher text is the same or smaller than the original plain text.	The size of cipher text is the same or larger than the original plain text.
The encryption process is very fast.	The encryption process is slow.
It is used when a large amount of data is required to transfer.	It is used to transfer small amounts of data.
It only provides confidentiality.	It provides confidentiality, authenticity, and non-repudiation.
The length of key used is 128 or 256 bits	The length of key used is 2048 or higher
In symmetric key encryption, resource utilization is low as compared to asymmetric key encryption.	In asymmetric key encryption, resource utilization is high.
It is efficient as it is used for handling large amount of data.	It is comparatively less efficient as it can handle a small amount of data.
Security is less as only one key is used for both encryption and decryption purpose.	It is more secure as two keys are used here- one for encryption and the other for decryption.
The Mathematical Representation is as follows- P = D (K, E(K, P)) where K –> encryption and decryption key P –> plain text D –> Decryption E(K, P) –> Encryption of plain text using K	The Mathematical Representation is as follows- P = D(Kd, E (Ke,P)) where Ke –> encryption key Kd –> decryption key D –> Decryption E(Ke, P) –> Encryption of plain text using encryption key Ke. P –> plain text
Examples: 3DES, AES, DES and RC4	Examples: Diffie-Hellman, ECC, El Gamal, DSA and RSA

Explain Diffie Hellman key exchange algorithm?

- Diffie-Hellman key exchange is a method of digital encryption that securely exchanges cryptographic keys between two parties over a public channel without their conversation being transmitted over the internet.
-
- The two parties use asymmetric cryptography to encrypt and decrypt their messages.



Example :


1 Alice & Bob agree upon 2 large prime numbers
n = 11
g = 7
Alice
Bob
2
x = 3
4
y = 6
A = g^x mod n
B = g^y mod n
A = 7^3 mod 11 = 2
5
B = 7^6 mod 11 = 4
B = 4
A = 2
6
K1 = B^x mod n
7
K2 = A^y mod n
K1 = 4^3 mod 11 = 9
K2 = 2^6 mod 11 = 9
K1 == K2