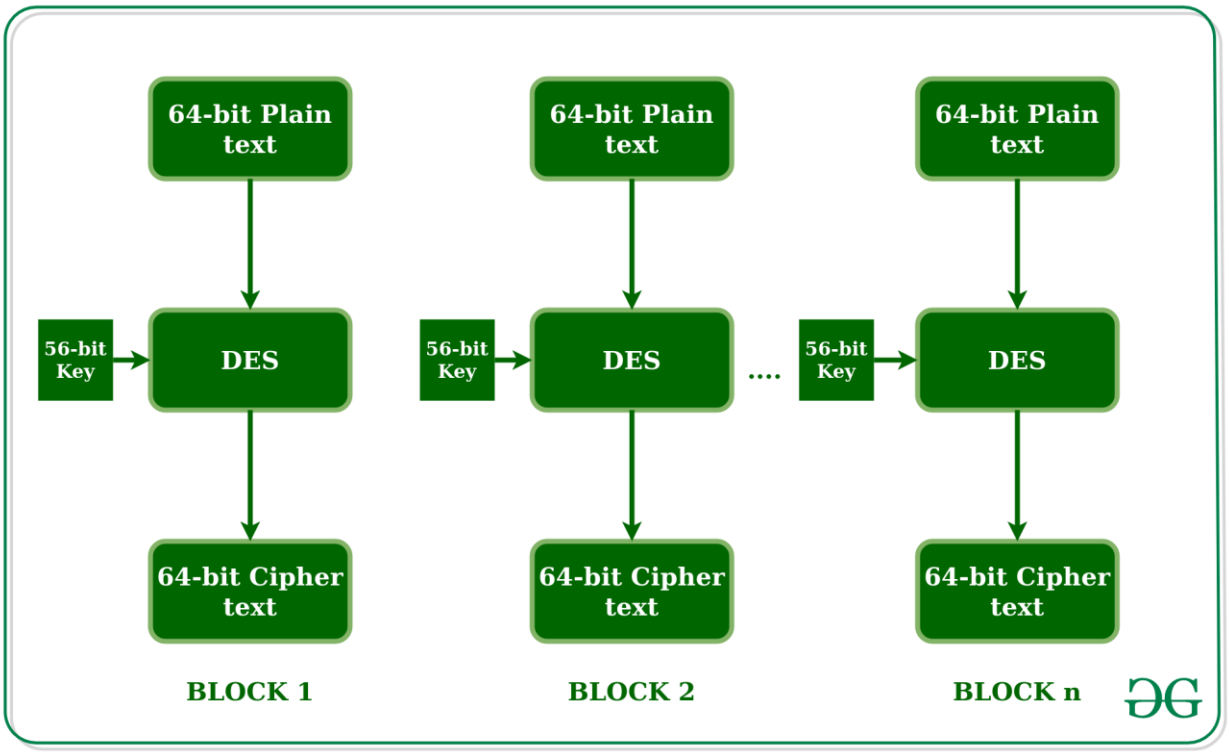
Unit- 3 Symmetric Key Encryption

Data Encryption Standard (DES) Algorithm:

Data encryption standard (DES) has been found vulnerable against 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 bit each, means 64 bits of plain text goes as the input to DES, which produces 64 bits of cipher text. 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.



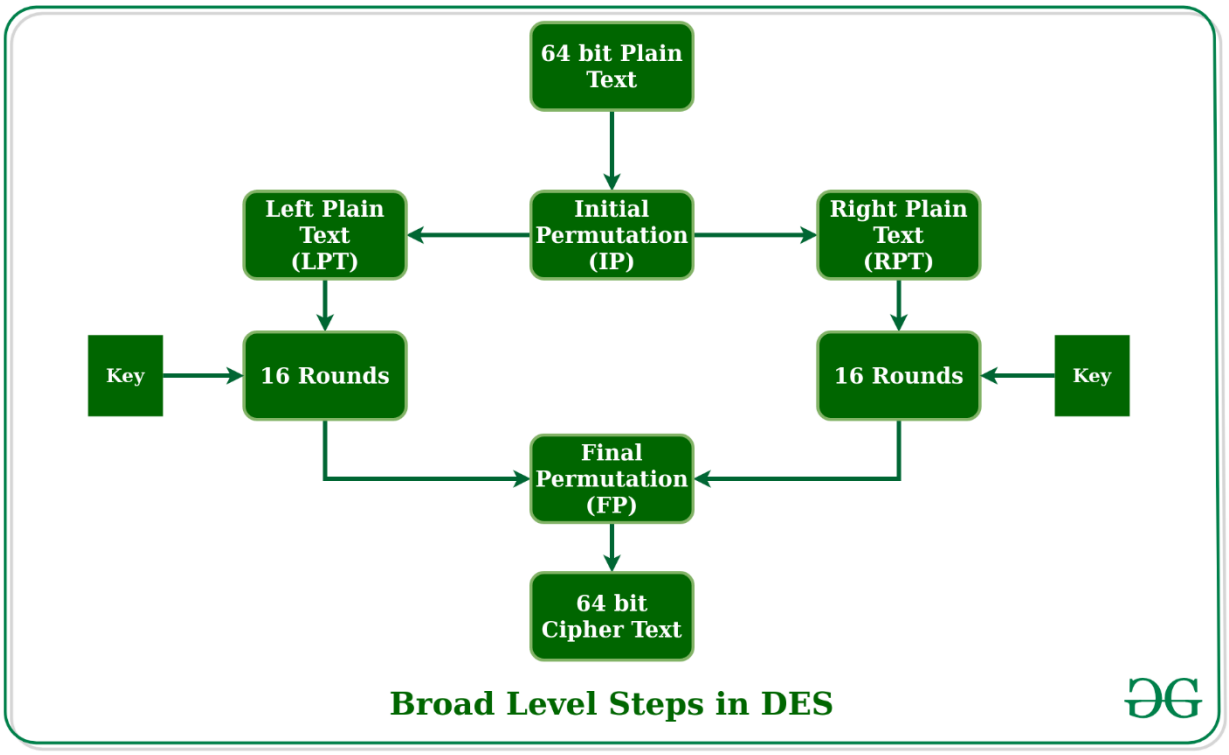
We have mentioned that DES uses a 56-bit key. Actually, the initial key consists of 64 bits. However, before the DES process even starts, every 8th bit of the key is discarded to produce a 56-bit key. That is bit position 8, 16, 24, 32, 40, 48, 56, and 64 are discarded.

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

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



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.

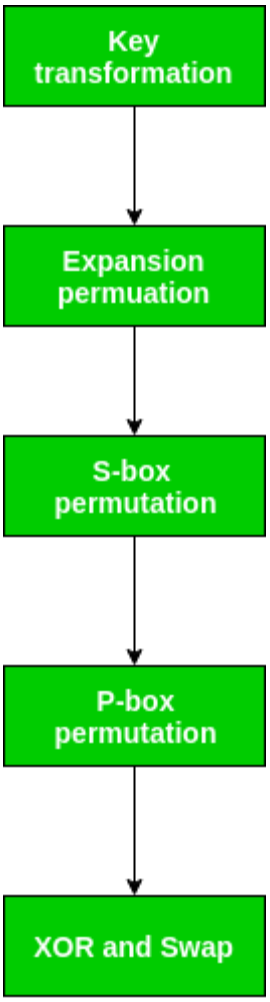
For example, it says that the IP replaces the first bit of the original plain text block with the 58th bit of the original plain text, the second bit with the 50th bit of the original plain text block, and so on.

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

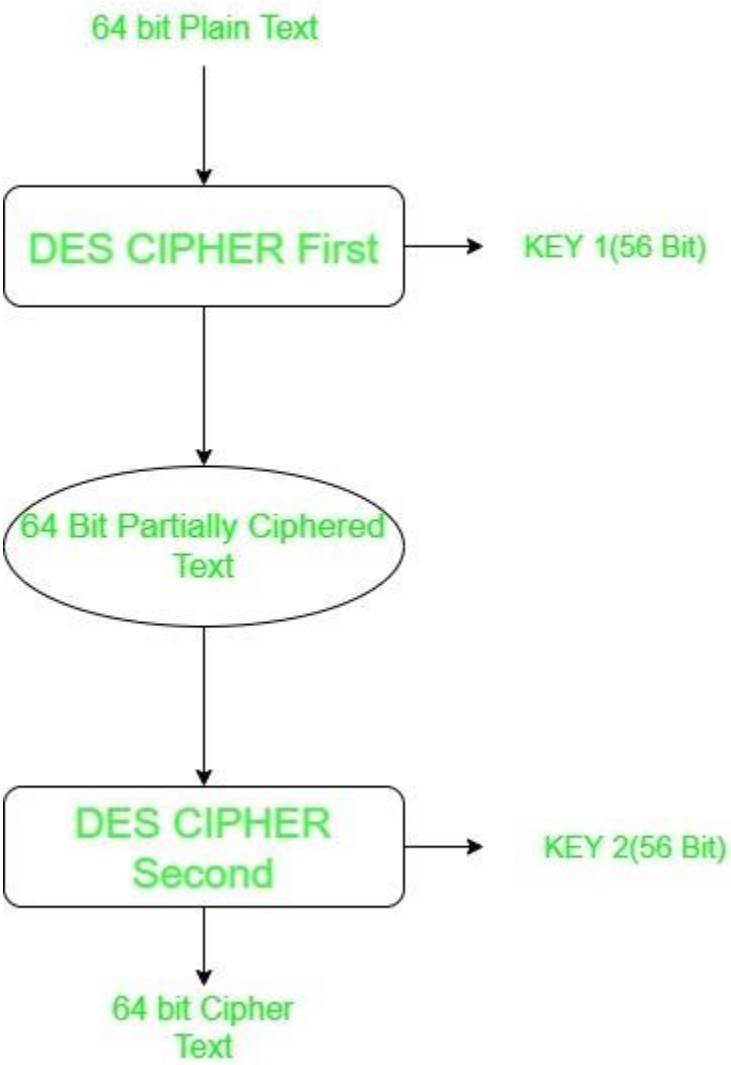
Figure - Initial permutation table

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.



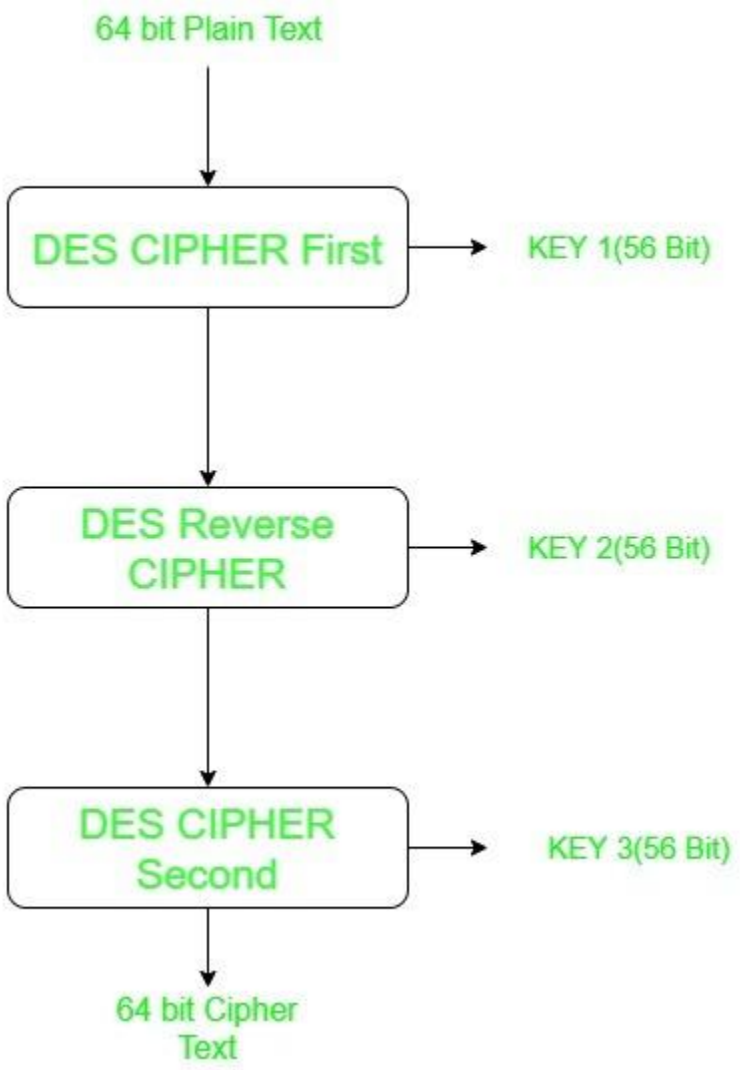
Double and Tripple DES:

Double DES:
Double DES is a encryption technique which uses two instance of DES on same plain text. In both instances it uses different keys to encrypt the plain text. Both keys are required at the time of decryption. The 64 bit plain text goes into first DES instance which than converted into a 64 bit middle text using the first key and then it goes to second DES instance which gives 64 bit cipher text by using second key.



However double DES uses 112 bit key but gives security level of 2^56 not 2^112 and this is because of meet-in-the middle attack which can be used to break through double DES.

Triple DES:
Triple DES is a encryption technique which uses three instance of DES on same plain text. It uses there different types of key choosing technique in first all used keys are different and in second two keys are same and one is different and in third all keys are same.



Triple DES is also vulnerable to meet-in-the middle attack because of which it give total security level of 2^112 instead of using 168 bit of key. The block collision attack can also be done because of short block size and using same key to encrypt large size of text. It is also vulnerable to sweet32 attack.

Security of the des:

A key size of 128 bits however this was reduced to 56 bits for **DES.** Even though **DES** actually accepts a 64 bit key as input, the remaining eight bits are used for parity checking and have no effect on **DES's security.** Outsiders were convinced that the 56 bit key was an easy target for a brute force attack4 due to its extremely small size.

Advanced Encryption Standard(AES) Algorithm:

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.
Points to remember

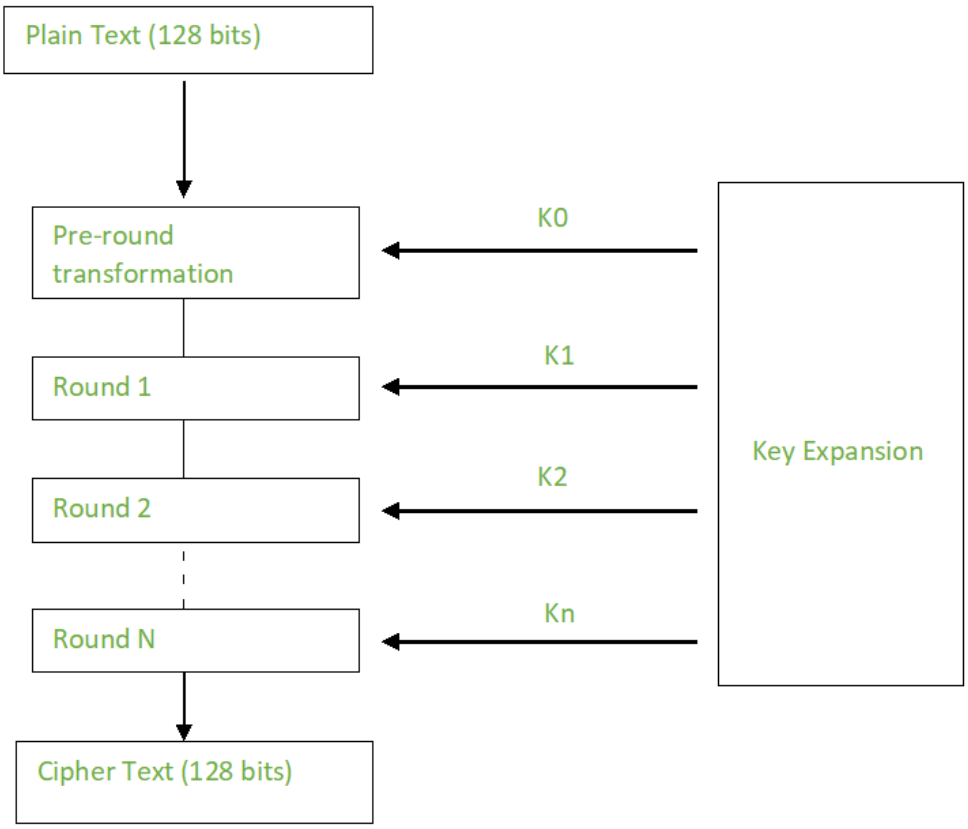
- AES is a block cipher.
- The key size can be 128/192/256 bits.
- Encrypts data in blocks of 128 bits each.

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. The 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.



DES AND AES Comparison:

AES	DES
AES stands for Advanced Encryption Standard	DES stands for Data Encryption Standard
The date of creation is 1999.	The date of creation is 1976.
Byte-Oriented.	Bit-Oriented.
Key length can be 128-bits, 192-bits, and 256-bits.	The key length is 56 bits in DES.

AES	DES
Number of rounds depends on key length: 10(128-bits), 12(192-bits), or 14(256-bits)	DES involves 16 rounds of identical operations
The structure is based on a substitution-permutation network.	The structure is based on a Feistel network.
The design rationale for AES is open.	The design rationale for DES is closed.
The selection process for this is secret but accepted open public comment.	The selection process for this is secret.
AES is more secure than the DES cipher and is the de facto world standard.	DES can be broken easily as it has known vulnerabilities. 3DES(Triple DES) is a variation of DES which is secure than the usual DES.
The rounds in AES are: Byte Substitution, Shift Row, Mix Column and Key Addition	The rounds in DES are: Expansion, XOR operation with round key, Substitution and Permutation
AES can encrypt 128 bits of plaintext.	DES can encrypt 64 bits of plaintext.
AES cipher is derived from an aside-channel square cipher.	DES cipher is derived from Lucifer cipher.
AES was designed by Vincent Rijmen and Joan Daemen.	DES was designed by IBM.

AES	DES
No known crypt-analytical attacks against AES but side channel attacks against AES implementations possible. Biclique attacks have better complexity than brute force but still ineffective.	Known attacks against DES include Brute-force, Linear crypt-analysis, and Differential crypt-analysis.

Characteristics of public key encryption :

Easy Key Management in Cryptography.

- Public Announcement: Here the public key is broadcasted to everyone. Major weakness of this method is forgery. Anyone can create a key claiming to be ...
- Publicly Available Directory: In this type, the public key is stored at a public directory. Directories are trusted here, with properties like ...
- Public Key Authority: It is similar to the directory but, improve security by tightening control over distribution of keys from directory. It requires ...
- Public Certification: This time authority provides a certificate (which binds identity to the public key) to allow key exchange without real-time ...

public key encryption

When the two parties communicate to each other to transfer the intelligible or sensible message, referred to as plaintext, is converted into apparently random nonsense for security purpose referred to as **ciphertext**.

Encryption:
The process of changing the plaintext into the ciphertext is referred to as **encryption.**
The encryption process consists of an algorithm and a key. The key is a value independent of the plaintext.

The security of conventional encryption depends on the major two factors:

1. The Encryption algorithm
2. Secrecy of the key

Once the ciphertext is produced, it may be transmitted. The Encryption algorithm will produce a different output depending on the specific key being used at the time. Changing the key changes the output of the algorithm.
Once the ciphertext is produced, it may be transmitted. Upon reception, the ciphertext can be transformed back to the original plaintext by using a decryption algorithm and the same key that was used for encryption.

Decryption:
The process of changing the ciphertext to the plaintext that process is known as **decryption**.

Public Key Encryption : Asymmetric is a form of Cryptosystem in which encryption and decryption are performed using different keys-Public key (known to everyone) and Private key (Secret key). This is known as **Public Key Encryption.**

Difference between Encryption and Public-key Encryption:

basis	**Encryption**	**Public-Key Encryption**
Required for Work:	• Same algorithm with the same key is used for encryption and decryption. • The sender and receiver must share the algorithm and key.	• One algorithm is used for encryption and a related algorithm decryption with pair of keys, one for encryption and other for decryption. • Receiver and Sender must each

RSA Techniques:

RSA Algorithm in Cryptography

RSA algorithm is asymmetric cryptography algorithm. Asymmetric actually means that it works on two different keys i.e. **Public Key** and **Private Key.** As the name describes that the Public Key is given to everyone and Private key is kept private.

An example of asymmetric cryptography :

1. A client (for example browser) sends its public key to the server and requests for some data.
2. The server encrypts the data using client's public key and sends the encrypted data.
3. Client receives this data and decrypts it.

Since this is asymmetric, nobody else except browser can decrypt the data even if a third party has public key of browser.

The idea! The idea of RSA is based on the fact that it is difficult to factorize a large integer. The public key consists of two numbers where one number is multiplication of two large prime numbers. And private key is also derived from the same two prime numbers. So if somebody can factorize the large number, the private key is compromised. Therefore encryption strength totally lies on the key size and if we double or triple the key size, the strength of encryption increases exponentially. RSA keys can be typically 1024 or 2048 bits long, but experts believe that 1024 bit keys could be broken in the near future. But till now it seems to be an infeasible task.

Let us learn the mechanism behind RSA algorithm :

>> Generating Public Key :

- Select two prime no's. Suppose **P = 53 and Q = 59**.
- Now First part of the Public key : **n = P*Q = 3127**.
-
- We also need a small exponent say **e** :
- But e Must be
  -
    - An integer.

-
- Not be a factor of n.
-
- **1 < e <** Φ(n) [Φ(n) is discussed below],
- Let us now consider it to be equal to 3.

-

- Our Public Key is made of n and e

>> Generating Private Key :

- We need to calculate Φ(n) :
- Such that **Φ(n) = (P-1)(Q-1)**
- so, Φ(n) = 3016
-
- Now calculate Private Key, **d** :
- **d = (k*Φ(n) + 1) / e** for some integer k
- For k = 2, value of d is 2011.

Now we are ready with our – Public Key (n = 3127 and e = 3) and Private Key(d = 2011)

Now we will encrypt **"HI"** :

- Convert letters to numbers : H = 8 and I = 9
- Thus **Encrypted Data c = 89^e mod n**.
- Thus our Encrypted Data comes out to be 1394

- Now we will decrypt **1394** :
- **Decrypted Data = c^d mod n**.
- Thus our Encrypted Data comes out to be 89
- **8 = H and I = 9 i.e. "HI".**

Key Exchange:

Internet Key Exchange (IKE) is a key management protocol standard used in conjunction with the Internet Protocol Security (IPSec) standard protocol. It provides security for virtual private networks' (VPNs) negotiations and network access to random hosts.

Diffie Hellman Scheme

The Diffie Hellman Algorithm is being used to **establish a shared secret** that can be used for secret communications while exchanging data over a public network. In the below program, the client will share the value of , , and public key . Whereas, the server will accept the values and calculate its public key and send it to the client.

Diffie-Hellman algorithm

The Diffie-Hellman algorithm is being used to establish a shared secret that can be used for secret communications while exchanging data over a public network using the elliptic curve to generate points and get the secret key using the parameters.

- For the sake of simplicity and practical implementation of the algorithm, we will consider only 4 variables, one prime P and G (a primitive root of P) and two private values a and b.
- P and G are both publicly available numbers. Users (say Alice and Bob) pick private values a and b and they generate a key and exchange it publicly. The opposite person receives the key and that generates a secret key, after which they have the same secret key to encrypt.

Step by Step Explanation

Alice	Bob
Public Keys available = P, G	Public Keys available = P, G
Private Key Selected = a	Private Key Selected = b
Key generated =	Key generated =

Exchange of generated keys takes place

Alice	Bob
Key received = y	key received = x
Generated Secret Key =	Generated Secret Key =

Algebraically, it can be shown that

Users now have a symmetric secret key to encrypt

Example:

Step 1: Alice and Bob get public numbers P = 23, G = 9

Step 2: Alice selected a private key a = 4 and

Bob selected a private key b = 3

Step 3: Alice and Bob compute public values

Alice: x =(9^4 mod 23) = (6561 mod 23) = 6

Bob: y = (9^3 mod 23) = (729 mod 23) = 16

Step 4: Alice and Bob exchange public numbers

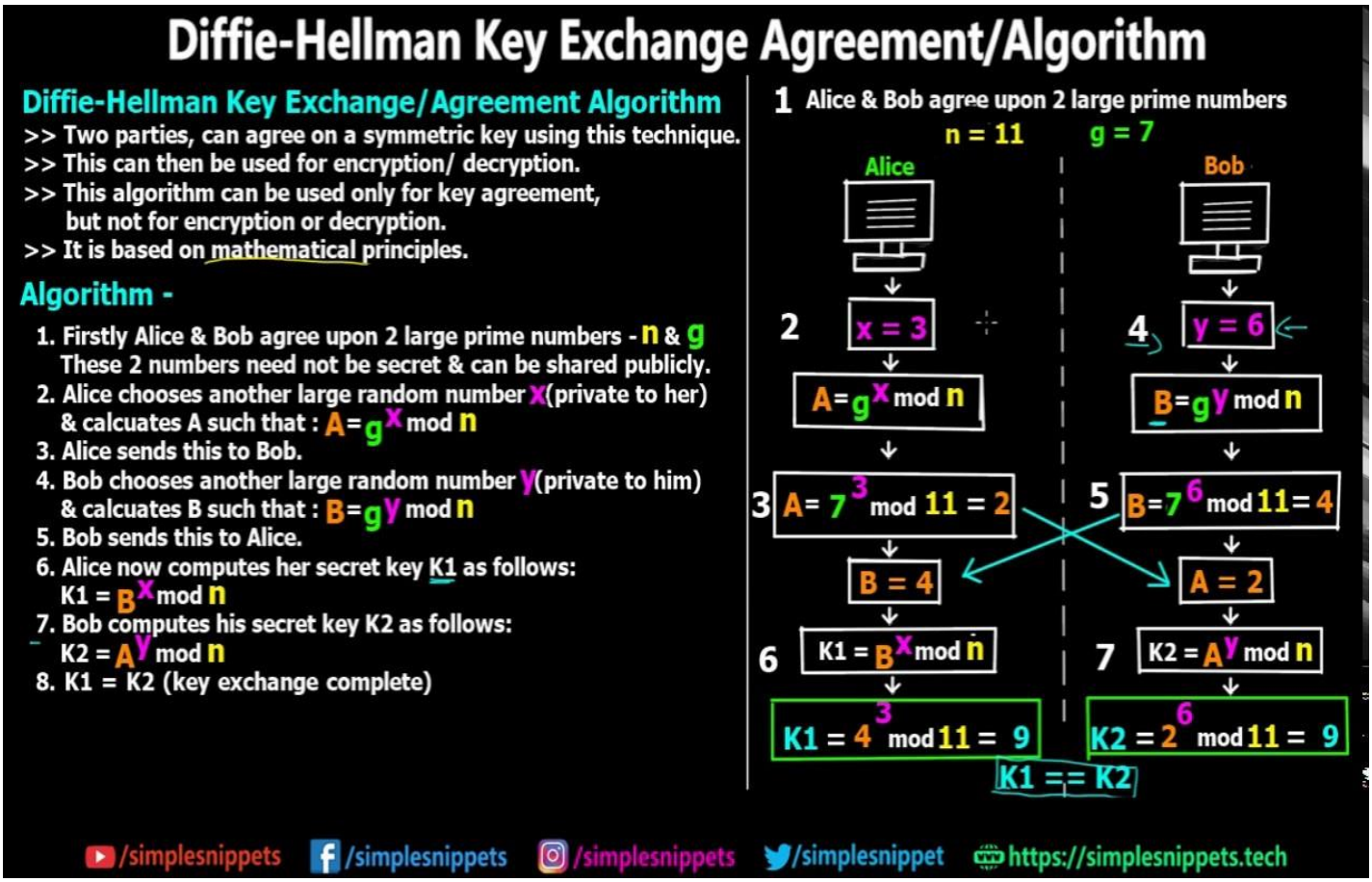
Step 5: Alice receives public key y =16 and

Bob receives public key x = 6

Step 6: Alice and Bob compute symmetric keys

Alice: ka = y^a mod p = 65536 mod 23 = 9

Bob: kb = x^b mod p = 216 mod 23 = 9



What is Cryptographic hash function?

A cryptographic hash function is a special class of hash function that has certain properties which make it suitable for use in cryptography. It is a mathematical algorithm that maps data of arbitrary size to a bit string of a fixed size (a hash function) which is designed to also be a one-way function, that is, a function which is infeasible to invert.

Digital Signatures and Certificates

Encryption – Process of converting electronic data into another form, called ciphertext, which cannot be easily understood by anyone except the authorized parties. This assures data security.
Decryption– Process of translating code to data.

- The message is encrypted at the sender's side using various encryption algorithms and decrypted at the receiver's end with the help of the decryption algorithms.
- When some message is to be kept secure like username, password, etc., encryption and decryption techniques are used to assure data security.

Types of Encryption

1. **Symmetric Encryption**– Data is encrypted using a key and the decryption is also done using the same key.
2. **Asymmetric Encryption**-Asymmetric Cryptography is also known as public-key cryptography. It uses public and private keys to encrypt and decrypt data. One key in the pair which can be shared with everyone is called the public key. The other key in the pair which is kept secret and is only known by the owner is called the private key. Either of the keys can be used to encrypt a message; the opposite key from the one used to encrypt the message is used for decryption.

Public key– Key which is known to everyone. Ex-public key of A is 7, this information is known to everyone.
Private key– Key which is only known to the person who's private key it is.
Authentication-Authentication is any process by which a system verifies the identity of a user who wishes to access it.
Non- repudiation– Non-repudiation means to ensure that a transferred message has been sent and received by the parties claiming to have sent and received the message. Non-repudiation is a way to guarantee that the sender of a message cannot later deny having sent the message and that the recipient cannot deny having received the message.
Integrity– to ensure that the message was not altered during the transmission.
Message digest -The representation of text in the form of a single string of digits, created using a formula called a one way hash function. Encrypting a message digest with a private key creates a digital signature which is an electronic means of authentication..

Digital Signature

A digital signature is a mathematical technique used to validate the authenticity and integrity of a message, software, or digital document.

1. **Key Generation Algorithms**: Digital signature is electronic signatures, which assure that the message was sent by a particular sender. While performing digital transactions authenticity and integrity should be assured, otherwise, the data can be altered or someone can also act as if he was the sender and expect a reply.
2. **Signing Algorithms**: To create a digital signature, signing algorithms like email programs create a one-way hash of the electronic data which is to be signed. The signing algorithm then encrypts the hash value using the private key (signature key). This encrypted hash along with other information like the hashing algorithm is the digital signature. This digital signature is appended with the data and sent to the verifier. The reason for encrypting the hash instead of the entire message or document is that a hash function converts any arbitrary input into a much shorter fixed-length value. This saves time as now instead of signing a long message a shorter hash value has to be signed and moreover hashing is much faster than signing.
3. **Signature Verification Algorithms** : Verifier receives Digital Signature along with the data. It then uses Verification algorithm to process on the digital signature and the public key (verification key) and generates some value. It also applies the same hash function on the received data and generates a hash value. Then the hash value and the output of the verification algorithm are compared. If they both are equal, then the digital signature is valid else it is invalid.

The steps followed in creating digital signature are :

1. Message digest is computed by applying hash function on the message and then message digest is encrypted using private key of sender to form the digital signature. (digital signature = encryption (private key of sender, message digest) and message digest = message digest algorithm(message)).
2. Digital signature is then transmitted with the message.(message + digital signature is transmitted)
3. Receiver decrypts the digital signature using the public key of sender.(This assures authenticity, as only sender has his private key so only sender can encrypt using his private key which can thus be decrypted by sender’s public key).
4. The receiver now has the message digest.
5. The receiver can compute the message digest from the message (actual message is sent with the digital signature).

6. The message digest computed by receiver and the message digest (got by decryption on digital signature) need to be same for ensuring integrity.

Message digest is computed using one-way hash function, i.e. a hash function in which computation of hash value of a message is easy but computation of the message from hash value of the message is very difficult.

Digital Certificate

Digital certificate is issued by a trusted third party which proves sender's identity to the receiver and receiver's identity to the sender.
A digital certificate is a certificate issued by a Certificate Authority (CA) to verify the identity of the certificate holder. The CA issues an encrypted digital certificate containing the applicant's public key and a variety of other identification information. Digital certificate is used to attach public key with a particular individual or an entity.

Digital certificate contains:-

1. Name of certificate holder.
2. Serial number which is used to uniquely identify a certificate, the individual or the entity identified by the certificate
3. Expiration dates.
4. Copy of certificate holder's public key.(used for decrypting messages and digital signatures)
5. Digital Signature of the certificate issuing authority.

Digital certificate is also sent with the digital signature and the message.

Digital certificate vs digital signature :

Digital signature is used to verify authenticity, integrity, non-repudiation ,i.e. it is assuring that the message is sent by the known user and not modified, while digital certificate is used to verify the identity of the user, maybe sender or receiver. Thus, digital signature and certificate are different kind of things but both are used for security. Most websites use digital certificate to enhance trust of

their users

Feature	Digital Signature	Digital Certificate
Basics / Definition	Digital signature is like a fingerprint or an attachment to a digital document that ensures its authenticity and integrity.	Digital certificate is a file that ensures holder's identity and provides security.
Process / Steps	Hashed value of original message is encrypted with sender's secret key to generate the digital signature.	It is generated by CA (Certifying Authority) that involves four steps: Key Generation, Registration, Verification, Creation.
Security Services	**Authenticity** of Sender, **integrity** of the document and **non-repudiation**.	It provides security and **authenticity** of certificate holder.
Standard	It follows Digital Signature Standard (DSS).	It follows X.509 Standard Format.

Certificate Authorities:

Registration authority act as a intermediate between end user and the certificate authority. It also assist in day to day task of certificate authority. Accepting and verifying the details of new user's registration. User key generation. Backups and recovery of key. Certificate cancellation.

Let's Encrypt has become one of the most important organizations for creating a secure Internet. Let's Encrypt is a free, automated, and open certificate authority (CA), run for the public's benefit, a service provided by the Internet Security Research Group (ISRG).

The end user request for a digital certificate and the request goes to the registration authority (R+A) which then assist the certificate authority (CA) to create the digital certificate. Registration authority act as a intermediate between end user and the certificate authority.

What is digital signature and how it works?

Digital signatures are a type of esignature based on the PKI standards. It ensures the contents of a message haven't been changed or altered in transit. Digital signature solution like Zoho Sign, helps you to sign documents online in compliance with country-specific and industry specific regulations.

The digital signature is simply **a small block of data that is attached to documents you sign.** It is generated from your digital ID, which includes both a private and public key. The private key is used to apply the signature to the document, while the public key is sent with the file. The public key contains encrypted code, also called a "hash," that verifies your identity. Digital signatures can be used.