UNIT-IV

What is encryption?

Encryption is the method by which information is converted into secret code that hides the information's true meaning. The science of encrypting and decrypting information is called *cryptography*.

In computing, unencrypted data is also known as *plaintext*, and encrypted data is called *ciphertext*. The formulas used to encode and decode messages are called *encryption algorithms,* or *ciphers*.

Symmetric Encryption?

- Symmetric encryption is a type of encryption where only one key (a secret key) is used to both encrypt and decrypt electronic data.
- The entities communicating via symmetric encryption must exchange the key so that it can be used in the decryption process.
- This encryption method differs from asymmetric encryption where a pair of keys - one public and one private - is used to encrypt and decrypt messages.
- By using symmetric encryption algorithms, data is "scrambled" so that it can't be understood by anyone who does not possess the secret key to decrypt it.
- Once the intended recipient who possesses the key has the message, the algorithm reverses its action so that the message is returned to its original readable form.
- The secret key that the sender and recipient both use could be a specific password/code or it can be random string of letters or numbers that have been generated by a secure random number generator (RNG).

There are two types of symmetric encryption algorithms:

1. **Block algorithms.** Set lengths of bits are encrypted in blocks of electronic data with the use of a specific secret key. As the data is being encrypted, the system holds the data in its memory as it waits for complete blocks.

2. **Stream algorithms.** Data is encrypted as it streams instead of being retained in the system's memory.

   Some examples of symmetric encryption algorithms include:

- AES (Advanced Encryption Standard)
- DES (Data Encryption Standard)
- IDEA (International Data Encryption Algorithm)
- Blowfish (Drop-in replacement for DES or IDEA)

What is DES?

Data Encryption Standard (DES) is a block cipher with a 56-bit key length that has played a significant role in data security**.** Data encryption standard (DES) has been found vulnerable to very powerful attacks 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 below:

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

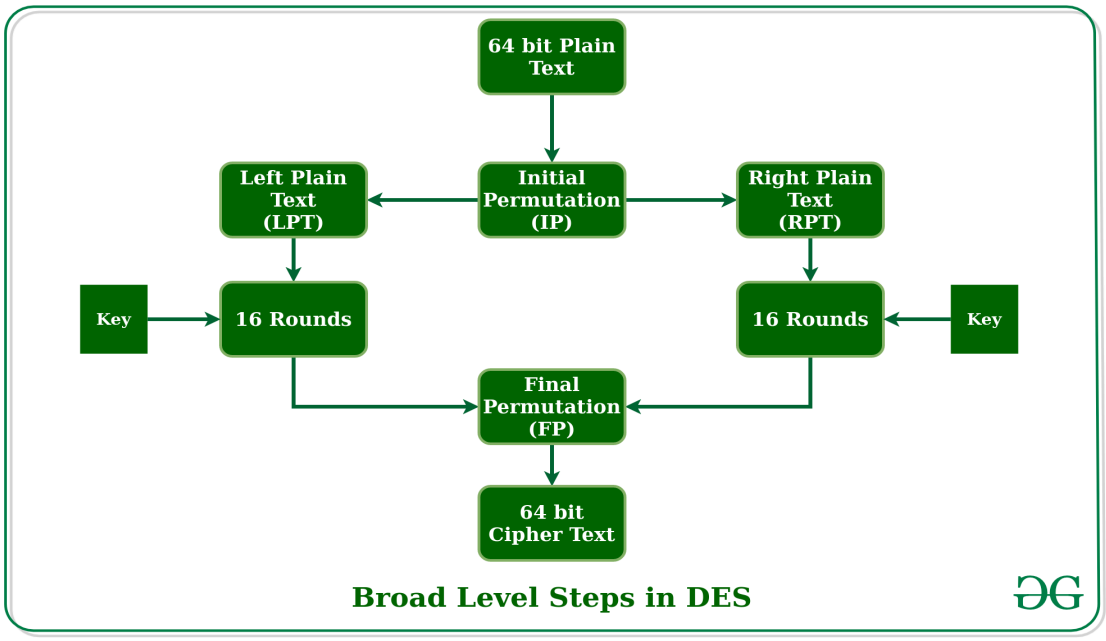
Figure - discording of every 8th bit of original key

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.



Broad Level Steps in DES

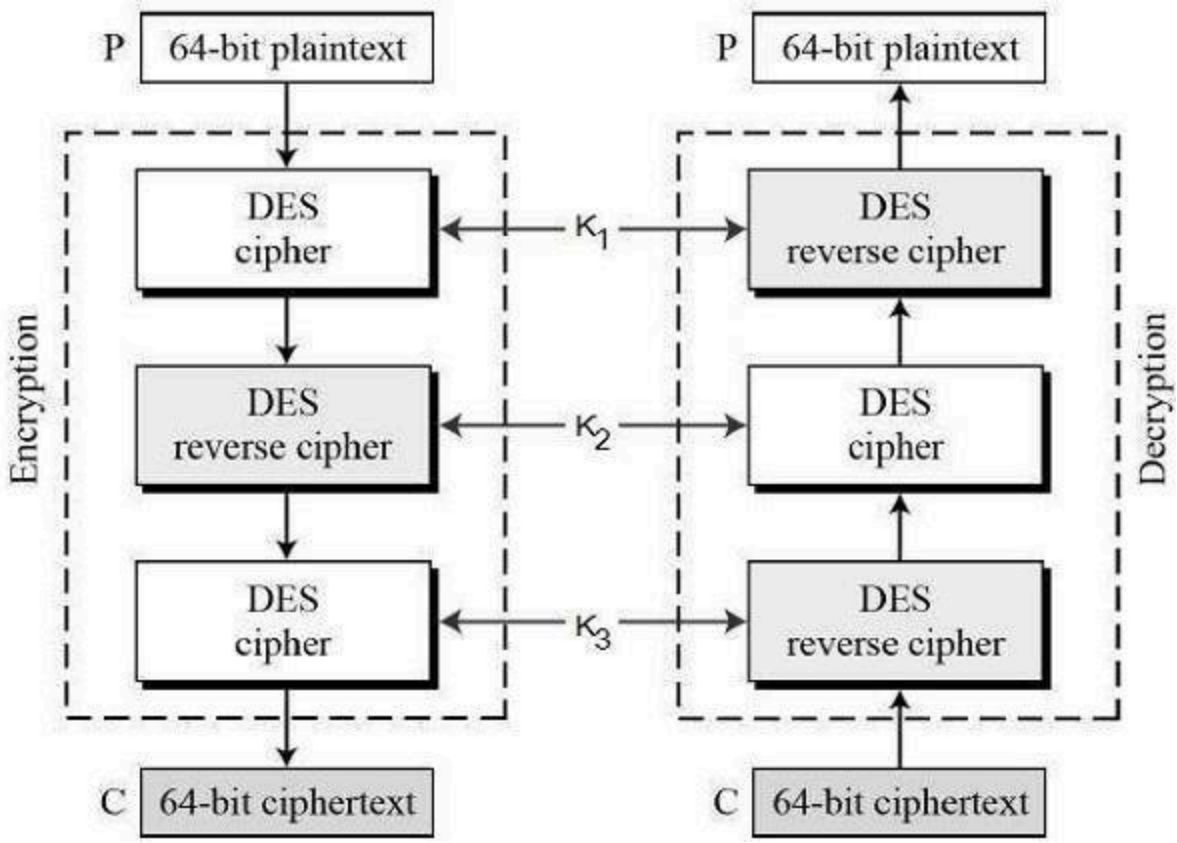
The speed of exhaustive key searches against DES after 1990 began to cause discomfort amongst users of DES. However, users did not want to replace DES as it takes an enormous amount of time and money to change encryption algorithms that are widely adopted and embedded in large security architectures.

The pragmatic approach was not to abandon the DES completely, but to change the manner in which DES is used. This led to the modified schemes of Triple DES (sometimes known as 3DES).

Incidentally, there are two variants of Triple DES known as 3-key Triple DES (3TDES) and 2-key Triple DES (2TDES).

3-KEY Triple DES

Before using 3TDES, user first generate and distribute a 3TDES key K, which consists of three different DES keys K_1, K_2 and K_3. This means that the actual 3TDES key has length $3\times56 = 168$ bits. The encryption scheme is illustrated as follows −



The encryption-decryption process is as follows −

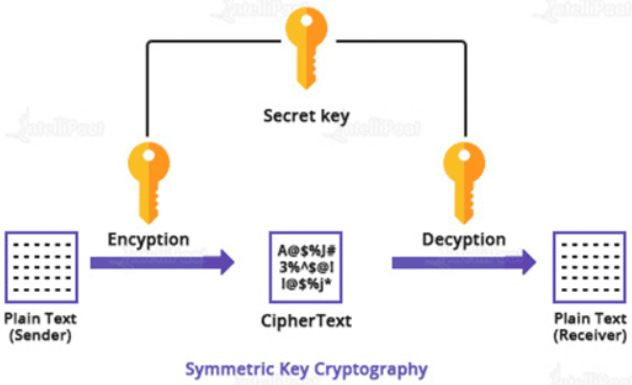
- Encrypt the plaintext blocks using single DES with key K_1.
- Now decrypt the output of step 1 using single DES with key K_2.
- Finally, encrypt the output of step 2 using single DES with key K_3.
- The output of step 3 is the ciphertext.
- Decryption of a ciphertext is a reverse process. User first decrypt using K_3, then encrypt with K_2, and finally decrypt with K_1.

Due to this design of Triple DES as an encrypt–decrypt–encrypt process, it is possible to use a 3TDES (hardware) implementation for single DES by setting K_1, K_2, and K_3 to be the same value. This provides backwards compatibility with DES.

Second variant of Triple DES (2TDES) is identical to 3TDES except that $K_3$is replaced by K_1. In other words, user encrypt plaintext blocks with key K_1, then decrypt with key K_2, and finally encrypt with K_1 again. Therefore, 2TDES has a key length of 112 bits.

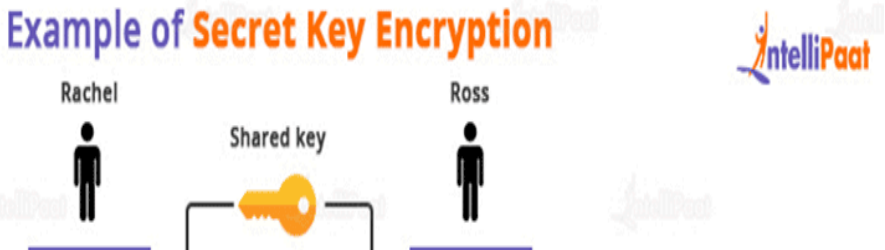
Triple DES systems are significantly more secure than single DES, but these are clearly a much slower process than encryption using single DES.

What is “Secret Key Cryptography”?



- A set of bits known as the secret key is used in secret key cryptography to decipher the plaintext message to be encrypted.
- The same key is employed to decipher the text message: that’s why it is also called a symmetric key.
- Since it is the first understandable message or piece of data delivered into the encryption process as input, the secret key is also a component of the encryption algorithm in cryptography.
- An algorithm value called the main, has nothing to do with plaintext. The method yields various results depending on the key. The method uses the secret to precise transformation and replacement.
- The same letter can have two different ciphertexts generated by two separate keys. Currently, the ciphertext is a stream of almost random data.

Secret Key Cryptography Examples



- A quick and easy way to encrypt texts is to swap out each letter for one from a different alphabetic letter. The quantity of places is crucial. The phrase “This is an example” can be encrypted with the key “1 position,” for instance, in the encrypted message “Uijt jt bo fybnqmf.” The original message would be repeated if the letter was taken one position higher in the alphabet.
- The stability of this apparatus is not great. There are just 26 potential keys in all. Only one key should be tried by Eve to determine which one generates a legible message. Furthermore, it is commonly known that some letters are used in communications more frequently than others.
- For instance, the letter “e” would be most frequently used in the English language. This fact might be used by Eve to count the number of times the letter “e” occurs in the encryption algorithm and change it with it. In particular, she is cognizant of how many spins are necessary to switch from “e” to the encoded counterpart of “e,” thus she can solve the problem right away.

Asymmetric Encryption?

- Asymmetric encryption, also known as public-key cryptography, is a type of encryption that uses a pair of keys to encrypt and decrypt data.
- The pair of keys includes a public key, which can be shared with anyone, and a private key, which is kept secret by the owner.
- In asymmetric encryption, the sender uses the recipient’s public key to encrypt the data. The recipient then uses their private key to decrypt the data. This approach allows for secure communication between two parties without the need for both parties to have the same secret key.

- Asymmetric encryption has several advantages over symmetric encryption, which uses the same key for both encryption and decryption.
- One of the main advantages is that it eliminates the need to exchange secret keys, which can be a challenging process, especially when communicating with multiple parties. Additionally, asymmetric encryption allows for the creation of digital signatures, which can be used to verify the authenticity of data.
- Asymmetric encryption is commonly used in various applications, including secure online communication, digital signatures, and secure data transfer.
- Asymmetric encryption is frequently used for secure internet communication, including email encryption, e-commerce, and online banking. Digital signatures, which are used to confirm the legitimacy of digital documents and messages, are another application for it.

Advantages of Asymmetric Encryption

Asymmetric encryption also known as public key cryptography is a method of cryptography that uses two different keys to encrypt and decrypt data, here are some advantages of asymmetric encryption: –

- **Enhanced Security:** Asymmetric encryption provides a higher level of security compared to symmetric encryption where only one key is used for both encryption and decryption with asymmetric encryption a different key is used for each process and the private key used for decryption is kept secret by the receiver making, it harder for an attacker to intercept and decrypt the data.
- **Authentication:** Asymmetric encryption can be used for authentication purposes which means that the receiver can verify the sender s identity. This is achieved by the sender encrypting a message with their private key which can only be decrypted with their public key if the receiver can successfully decrypt the message, it proves that it was sent by the sender who has the corresponding private key.
- **Non-repudiation:** Asymmetric encryption also provides non-repudiation which means that the sender cannot deny sending a message or altering its contents this is because the message is encrypted with the sender s private key and only their public key can decrypt it . Therefore, the receiver can be sure that the message was sent by the sender and has not been tampered with.
- **Key distribution:** Asymmetric encryption eliminates the need for a secure key distribution system that is required in symmetric encryption with symmetric

encryption, the same key is used for both encryption and decryption and the key needs to be securely shared between the sender and the receiver asymmetric encryption, on the other hand, allows the public key to be shared openly and the private key is kept secret by the receiver.

- **Versatility:** Asymmetric encryption can be used for a wide range of applications including secure email communication online banking transactions and e-commerce it is also used to secure SSL/TSL connections which are commonly used to secure internet traffic.

Public Key Encryption

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**

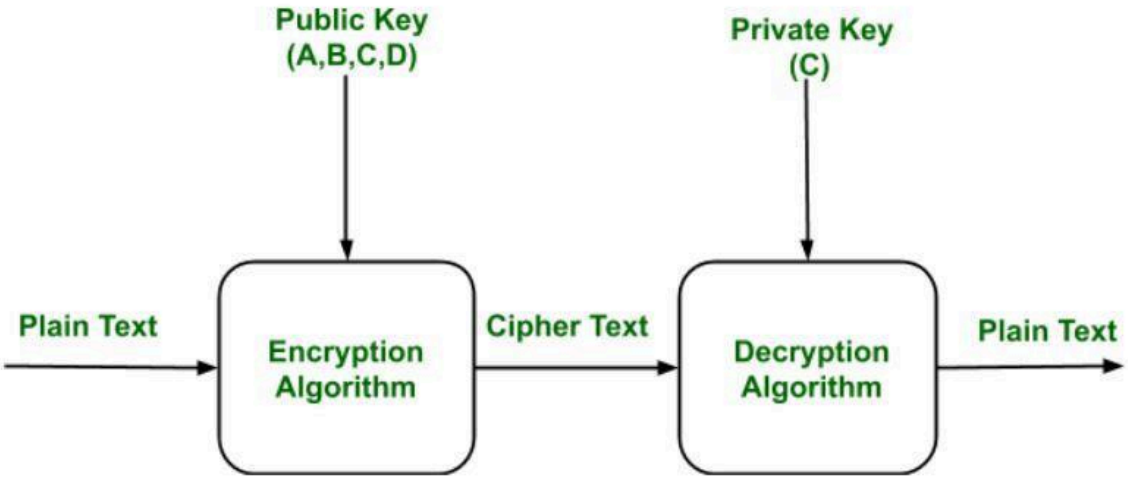
Required for Work:	• Same algorithm with the same key is used for encryption and decryption. • The sender and receiver must share the algorithm and key.	• One algorithm is used for encryption and a related algorithm decryption with pair of keys, one for encryption and other for decryption. • Receiver and Sender must each have one of the matched pair of keys (not identical) .
Required for Security:	• Key must be kept secret. • If the key is secret, it is very impossible to decipher message. • Knowledge of the algorithm plus samples of ciphertext must be impractical to determine the key.	• One of the two keys must be kept secret. • If one of the key is kept secret, it is very impossible to decipher message. • Knowledge of the algorithm plus one of the keys plus samples of ciphertext must be impractical to determine the other key.

Characteristics of Public Encryption key:

- Public key Encryption is important because it is infeasible to determine the decryption key given only the knowledge of the cryptographic algorithm and encryption key.
- Either of the two keys (Public and Private key) can be used for encryption with other key used for decryption.
- Due to Public key cryptosystem, public keys can be freely shared, allowing users an easy and convenient method for encrypting content and verifying digital signatures, and private keys can be kept secret, ensuring only the owners of the private keys can decrypt content and create digital signatures.
- The most widely used public-key cryptosystem is RSA (Rivest–Shamir–Adleman). The difficulty of finding the prime factors of a composite number is the backbone of RSA.

Example:

Public keys of every user are present in the Public key Register. If B wants to send a confidential message to C, then B encrypt the message using C Public key. When C receives the message from B then C can decrypt it using its own Private key. No other recipient other than C can decrypt the message because only C know C's private key.



Components of Public Key Encryption:

- **Plain Text:**
  This is the message which is readable or understandable. This message is given to the Encryption algorithm as an input.
- **Cipher Text:**
  The cipher text is produced as an output of Encryption algorithm. We cannot simply understand this message.
- **Encryption Algorithm:**
  The encryption algorithm is used to convert plain text into cipher text.
- **Decryption Algorithm:**
  It accepts the cipher text as input and the matching key (Private Key or Public key) and produces the original plain text
- **Public and Private Key:**
  One key either Private key (Secret key) or Public Key (known to everyone) is used for encryption and other is used for decryption

Weakness of the Public Key Encryption:

- Public key Encryption is vulnerable to Brute-force attack.
- This algorithm also fails when the user lost his private key, then the Public key Encryption becomes the most vulnerable algorithm.
- Public Key Encryption also is weak towards man in the middle attack. In this attack a third party can disrupt the public key communication and then modify the public keys.
- If user private key used for certificate creation higher in the PKI(Public Key Infrastructure) server hierarchy is compromised, or accidentally disclosed, then a “man-in-the-middle attack” is also possible, making any subordinate certificate wholly insecure. This is also the weakness of public key Encryption.

Applications of the Public Key Encryption:

- **Encryption/Decryption:**
  Confidentiality can be achieved using Public Key Encryption. In this the Plain text is encrypted using receiver public key. This will ensure that no one other than receiver private key can decrypt the cipher text.
- **Digital signature:**
  Digital signature is for senders authentication purpose. In this sender encrypt the plain text using his own private key. This step will make sure the authentication of the sender because receiver can decrypt the cipher text using senders public key only.
- **Key exchange:**
  This algorithm can use in both Key-management and securely transmission of data.

What is a private key?

A private key, also known as a *secret key*, is a variable in cryptography that is used with an algorithm to encrypt and decrypt data. Secret keys should only be shared with the key's generator or parties authorized to decrypt the data. Private keys play an important role in symmetric cryptography, asymmetric cryptography and cryptocurrencies.

DIGITAL SIGNATURE

MAC(Message Authentication Code) was used to provide Message Integrity and Message Authentication but it needs symmetric key established between sender and receiver. A digital signature on other hand uses pair of asymmetric keys.

A valid digital signature helps the receiver to know the message comes from the authentic sender and is not altered in between.

What is a Signature?

We sign a document to show that is approved by us or created by us. The signature is proof to the recipient that this document is coming from the correct source. The signature on the document simply means the document is authentic.

When A sends a message to B, B needs to check the authenticity of the message and confirm it comes from A and not C. So B can ask A to sign the message electronically. The electronic signature proves the identity of A is also called a digital signature.

Conventional Signature Vs Digital Signature

Conventional Signature	**Digital Signature**
A conventional Signature is part of a document. For example, when we sign a cheque the signature is present on the cheque not on a separate document.	A digital signature is not part of a document. This means the sender sends two documents message and signature.
To verify conventional signatures the recipient compares the signature on the document with the signature on file. So recipient needs to have a copy of this signature on file for comparison.	To verify digital signatures the recipient applies verification technique to a combination of message and the signature to verify authenticity. So here a copy of the signature is not stored anywhere.
the One to Many relationships between document and signature.	One to One relationship between message and signature. Every message has its own signature.
Copy of signed document can be distinguished from the original signature on file.	No distinction can be made unless there is a factor of time(timestamp) on the document.

VIRTUAL PRIVATE NETWORK[VPN]

VPN stands for the **Virtual Private Network**. A virtual private network (VPN) is a technology that creates a safe and encrypted connection over a less secure network, such as the Internet. A Virtual Private Network is a way to extend a private network using a public network such as the Internet. The name only suggests that it is a Virtual "private network,**i.e., a**" i.e. user can be part of a local network sitting at a remote location. It makes use of tunneling protocols to establish a secure connection.

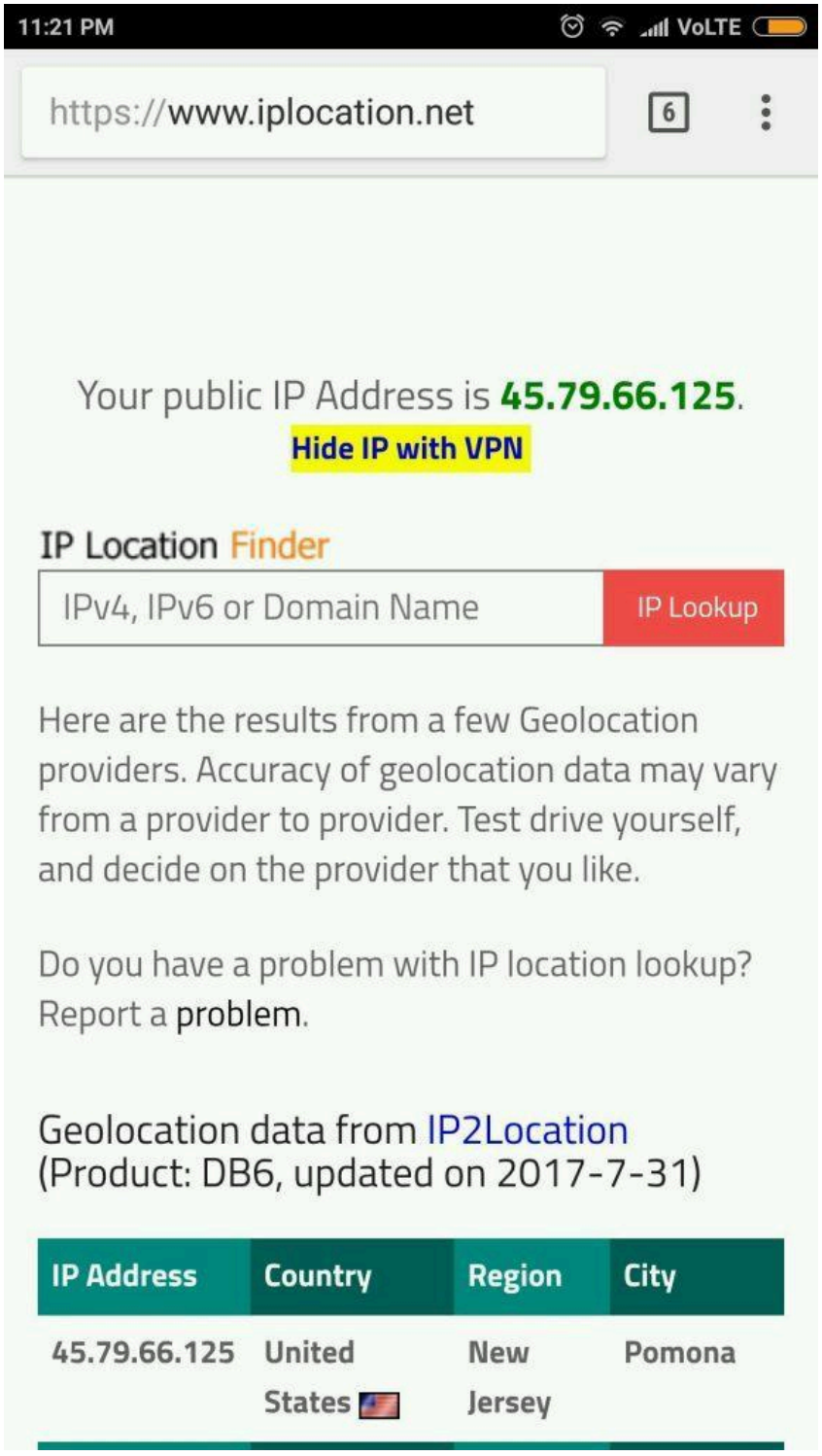
How does a VPN work?

Let us understand VPN with **Let's** an example

Think of a situation where the corporate office of a bank is situated in Washington, USA. This office has a local network consisting of say 100 computers. Suppose other branches of the bank are in Mumbai, India, and Tokyo, Japan. The traditional method of establishing a secure connection between the head office and the **the** branch was to have a leased line between the branches and head office which was a very costly as well as troublesome job. VPN lets us overcome this issue in an effective manner.

The situation is described below

- All 100 hundred computers of the corporate office at Washington are connected to the VPN server(which is a well-configured server containing a public IP address and a switch to connect all computers present in the local network i.e. in US head office).
- The person sitting in the Mumbai office connects to The VPN server using a dial-up window and the VPN server returns an IP address that belongs to the series of IP addresses belonging to a local network of the corporate office.
- Thus person from the Mumbai branch becomes local to the head office and information can be shared securely over the public internet.
- So this is the intuitive way of extending the local network even across the geographical borders of the country.



IP address changed to an IP address belonging to USA

1. VPN also ensures security by providing an encrypted tunnel between client and VPN server.
2. VPN is used to bypass many blocked sites.

3. VPN facilitates Anonymous browsing by hiding your ip address.
4. Also, most appropriate Search engine optimization(SEO) is done by analyzing the data from VPN providers which provide country-wise stats of browsing a particular product. This method of SEO is used widely my many internet marketing managers to form new strategies.
5. VPNs encrypt your internet traffic, safeguarding your online activities from potential eavesdropping and cyber threats, thereby enhancing your privacy and data protection.