**Computer Network Security**

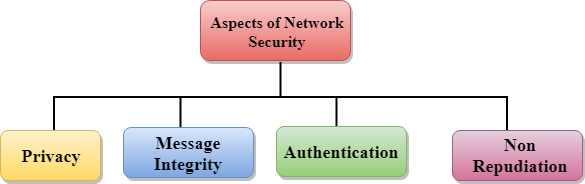
Computer network security consists of measures taken by business or some organizations to monitor and prevent unauthorized access from the outside attackers.

Different approaches to computer network security management have different requirements depending on the size of the computer network. For example, a home office requires basic network security while large businesses require high maintenance to prevent the network from malicious attacks.

Network Administrator controls access to the data and software on the network. A network administrator assigns the user ID and password to the authorized person.

## Aspects of Network Security:

Following are the desirable properties to achieve secure communication:



* **Privacy:** Privacy means both the sender and the receiver expects confidentiality. The transmitted message should be sent only to the intended receiver while the message should be opaque for other users. Only the sender and receiver should be able to understand the transmitted message as eavesdroppers can intercept the message. Therefore, there is a requirement to encrypt the message so that the message cannot be intercepted. This aspect of confidentiality is commonly used to achieve secure communication.
* **Message Integrity:** Data integrity means that the data must arrive at the receiver exactly as it was sent. There must be no changes in the data content during transmission, either maliciously or accident, in a transit. As there are more and more monetary exchanges over the internet, data integrity is more crucial. The data integrity must be preserved for secure communication.
* **End-point authentication:** Authentication means that the receiver is sure of the sender?s identity, i.e., no imposter has sent the message.
* **Non-Repudiation:** Non-Repudiation means that the receiver must be able to prove that the received message has come from a specific sender. The sender must not deny sending a message that he or she send. The burden of proving the identity comes on the receiver. For example, if a customer sends a request to transfer the money from one account to another account, then the bank must have a proof that the customer has requested for the transaction.

# Privacy

The concept of how to achieve privacy has not been changed for thousands of years: the message cannot be encrypted. The message must be rendered as opaque to all the unauthorized parties. A good encryption/decryption technique is used to achieve privacy to some extent. This technique ensures that the eavesdropper cannot understand the contents of the message.

## Encryption/Decryption

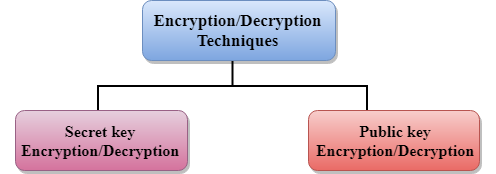
**Encryption:** Encryption means that the sender converts the original information into another form and sends the unintelligible message over the network.

**Decryption:** Decryption reverses the Encryption process in order to transform the message back to the original form.

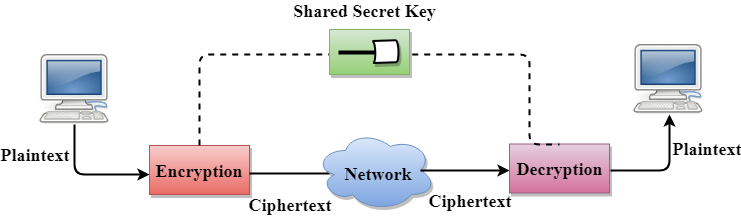
The data which is to be encrypted at the sender site is known as plaintext, and the encrypted data is known as ciphertext. The data is decrypted at the receiver site.

**There are two types of Encryption/Decryption techniques:**

* Privacy with secret key Encryption/Decryption
* Privacy with public key Encryption/Decryption



## Secret Key Encryption/Decryption technique



* In Secret Key Encryption/Decryption technique, the same key is used by both the parties, i.e., the sender and receiver.
* The sender uses the secret key and encryption algorithm to encrypt the data; the receiver uses this key and decryption algorithm to decrypt the data.
* In Secret Key Encryption/Decryption technique, the algorithm used for encryption is the inverse of the algorithm used for decryption. It means that if the encryption algorithm uses a combination of addition and multiplication, then the decryption algorithm uses a combination of subtraction and division.
* The secret key encryption algorithm is also known as symmetric encryption algorithm because the same secret key is used in bidirectional communication.
* In secret key encryption/decryption algorithm, the secret code is used by the computer to encrypt the information before it is sent over the network to another computer.
* The secret key requires that we should know which computers are talking to each other so that we can install the key on each computer.

### Data Encryption Standard (DES)

* The Data Encryption Standard (DES) was designed by IBM and adopted by the U.S. government as the standard encryption method for nonmilitary and nonclassified use.
* The Data Encryption Standard is a standard used for encryption, and it is a form of Secret **Key Cryptography**.

### Advantage

**Efficient:** The secret key algorithms are more efficient as it takes less time to encrypt the message than to encrypt the message by using a public key encryption algorithm. The reason for this is that the size of the key is small. Due to this reason, Secret Key Algorithms are mainly used for encryption and decryption.

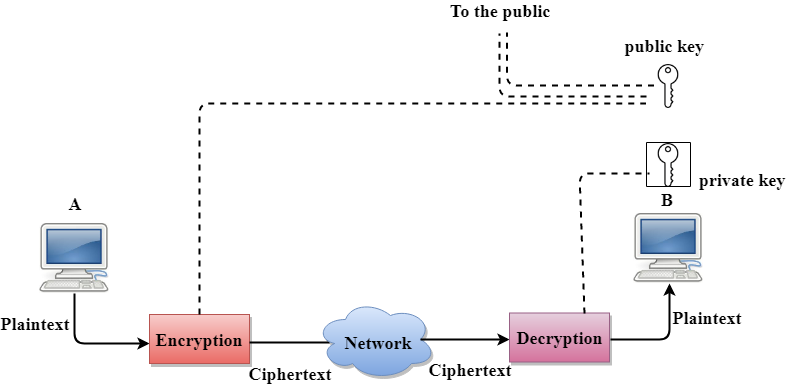
### Disadvantages of Secret Key Encryption

**The Secret Key Encryption/Decryption has the following disadvantages:**

* Each pair of users must have a secret key. If the number of people wants to use this method in the world is N, then there are N(N-1)/2 secret keys. For example, for one million people, then there are half billion secret keys.
* The distribution of keys among different parties can be very difficult. This problem can be resolved by combining the Secret Key Encryption/Decryption with the Public Key Encryption/Decryption algorithm.

## Public Key Encryption/Decryption technique

* There are two keys in public key encryption: a private key and a public key.
* The private key is given to the receiver while the public key is provided to the public.



In the above figure, we see that A is sending the message to user B. 'A' uses the public key to encrypt the data while 'B' uses the private key to decrypt the data.

* In public key Encryption/Decryption, the public key used by the sender is different from the private key used by the receiver.
* The public key is available to the public while the private key is kept by each individual.
* The most commonly used public key algorithm is known as RSA.

### Advantages of Public Key Encryption

* The main restriction of private key encryption is the sharing of a secret key. A third party cannot use this key. In public key encryption, each entity creates a pair of keys, and they keep the private one and distribute the public key.
* The number of keys in public key encryption is reduced tremendously. For example, for one million users to communicate, only two million keys are required, not a half-billion keys as in the case of secret key encryption.

### Disadvantages of Public Key Encryption

* **Speed:** One of the major disadvantage of the public-key encryption is that it is slower than secret-key encryption. In secret key encryption, a single shared key is used to encrypt and decrypt the message which speeds up the process while in public key encryption, different two keys are used, both related to each other by a complex mathematical process. Therefore, we can say that encryption and decryption take more time in public key encryption.
* **Authentication:** A public key encryption does not have a built-in authentication. Without authentication, the message can be interpreted or intercepted without the user's knowledge.
* **Inefficient:** The main disadvantage of the public key is its complexity. If we want the method to be effective, large numbers are needed. But in public key encryption, converting the plaintext into ciphertext using long keys takes a lot of time. Therefore, the public key encryption algorithms are efficient for short messages not for long messages.

## Differences b/w Secret Key Encryption & Public Key Encryption

|  |  |  |
| --- | --- | --- |
| **Basis for Comparison** | **Secret Key Encryption** | **Public Key Encryption** |
| Define | Secret Key Encryption is defined as the technique that uses a single shared key to encrypt and decrypt the message. | Public Key Encryption is defined as the technique that uses two different keys for encryption and decryption. |
| Efficieny | It is efficient as this technique is recommended for large amounts of text. | It is inefficient as this technique is used only for short messages. |
| Other name | It is also known as Symmetric Key encryption. | It is also known as Asymmetric Key Encryption. |
| Speed | Its speed is high as it uses a single key for encryption and decryption. | Its speed is slow as it uses two different keys, both keys are related to each other through the complicated mathematical process. |
| Algorithms | The Secret key algorithms are DES, 3DES, AES & RCA. | The Public key algorithms are Diffie-Hellman, RSA. |
| Purpose | The main purpose of the secret key algorithm is to transmit the bulk data. | The main purpose of the public key algorithm is to share the keys securely. |

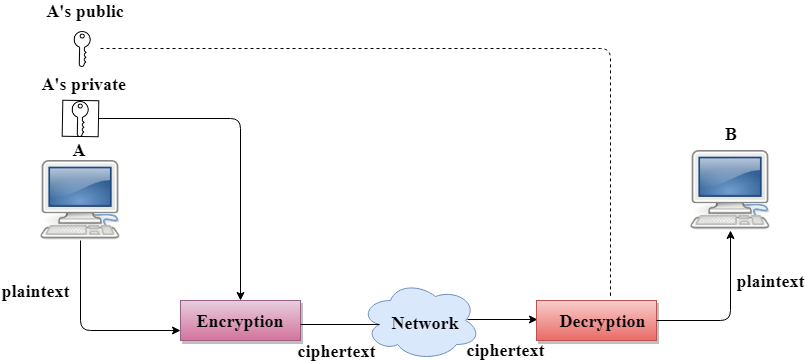
# Digital Signature

The Digital Signature is a technique which is used to validate the authenticity and integrity of the message. We know that there are four aspects of security: privacy, authentication, integrity, and non-repudiation. We have already discussed the first aspect of security and other three aspects can be achieved by using a digital signature.

The basic idea behind the Digital Signature is to sign a document. When we send a document electronically, we can also sign it. We can sign a document in two ways: to sign a whole document and to sign a digest.

## Signing the Whole Document

* In Digital Signature, a public key encryption technique is used to sign a document. However, the roles of a public key and private key are different here. The sender uses a private key to encrypt the message while the receiver uses the public key of the sender to decrypt the message.
* In Digital Signature, the private key is used for encryption while the public key is used for decryption.
* Digital Signature cannot be achieved by using secret key encryption.



### Digital Signature is used to achieve the following three aspects:

* **Integrity:** The Digital Signature preserves the integrity of a message because, if any malicious attack intercepts a message and partially or totally changes it, then the decrypted message would be impossible.
* **Authentication:** We can use the following reasoning to show how the message is authenticated. If an intruder (user X) sends a message pretending that it is coming from someone else (user A), user X uses her own private key to encrypt the message. The message is decrypted by using the public key of user A. Therefore this makes the message unreadable. Encryption with X's private key and decryption with A's public key results in garbage value.
* **Non-Repudiation:** Digital Signature also provides non-repudiation. If the sender denies sending the message, then her private key corresponding to her public key is tested on the plaintext. If the decrypted message is the same as the original message, then we know that the sender has sent the message.

#### Note: Digital Signature does not provide privacy. If there is a need for privacy, then another layer of encryption/decryption is applied.

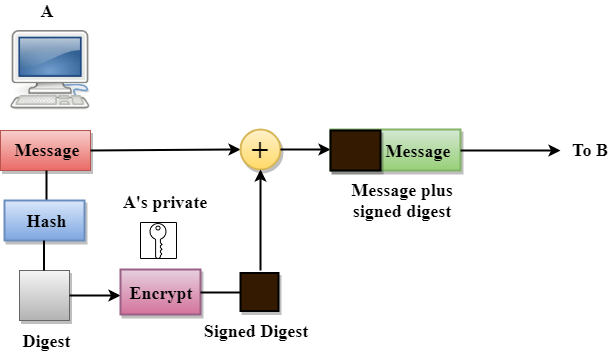
## Signing the Digest

* Public key encryption is efficient if the message is short. If the message is long, a public key encryption is inefficient to use. The solution to this problem is to let the sender sign a digest of the document instead of the whole document.
* The sender creates a miniature version (digest) of the document and then signs it, the receiver checks the signature of the miniature version.
* The hash function is used to create a digest of the message. The hash function creates a fixed-size digest from the variable-length message.
* The two most common hash functions used: MD5 (Message Digest 5) and SHA-1 (Secure Hash Algorithm 1). The first one produces 120-bit digest while the second one produces a 160-bit digest.
* A hash function must have two properties to ensure the success:
  + First, the digest must be one way, i.e., the digest can only be created from the message but not vice versa.
  + Second, hashing is a one-to-one function, i.e., two messages should not create the same digest.

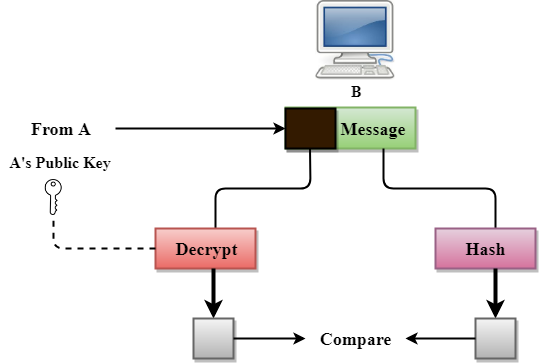
### Following are the steps taken to ensure security:

* The miniature version (digest) of the message is created by using a hash function.
* The digest is encrypted by using the sender's private key.
* After the digest is encrypted, then the encrypted digest is attached to the original message and sent to the receiver.
* The receiver receives the original message and encrypted digest and separates the two. The receiver implements the hash function on the original message to create the second digest, and it also decrypts the received digest by using the public key of the sender. If both the digests are same, then all the aspects of security are preserved.

**At the Sender site**



**At the Receiver site**



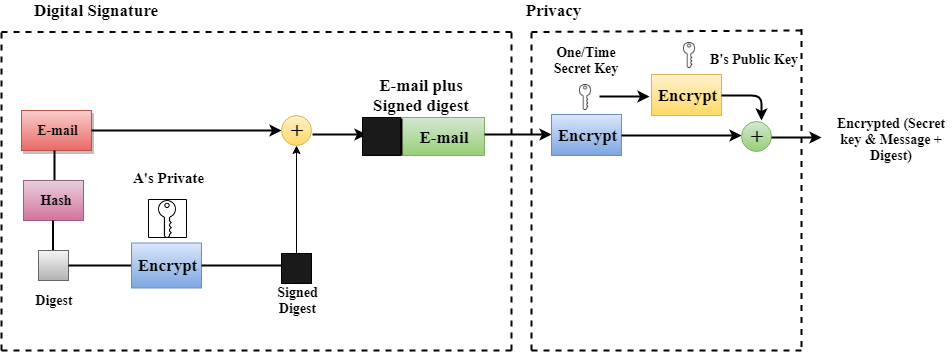
# PGP

* PGP stands for Pretty Good Privacy (PGP) which is invented by Phil Zimmermann.
* PGP was designed to provide all four aspects of security, i.e., privacy, integrity, authentication, and non-repudiation in the sending of email.
* PGP uses a digital signature (a combination of hashing and public key encryption) to provide integrity, authentication, and non-repudiation. PGP uses a combination of secret key encryption and public key encryption to provide privacy. Therefore, we can say that the digital signature uses one hash function, one secret key, and two private-public key pairs.
* PGP is an open source and freely available software package for email security.
* PGP provides authentication through the use of Digital Signature.
* It provides confidentiality through the use of symmetric block encryption.
* It provides compression by using the ZIP algorithm, and EMAIL compatibility using the radix-64 encoding scheme.

### Following are the steps taken by PGP to create secure e-mail at the sender site:

* The e-mail message is hashed by using a hashing function to create a digest.
* The digest is then encrypted to form a signed digest by using the sender's private key, and then signed digest is added to the original email message.
* The original message and signed digest are encrypted by using a one-time secret key created by the sender.
* The secret key is encrypted by using a receiver's public key.
* Both the encrypted secret key and the encrypted combination of message and digest are sent together.

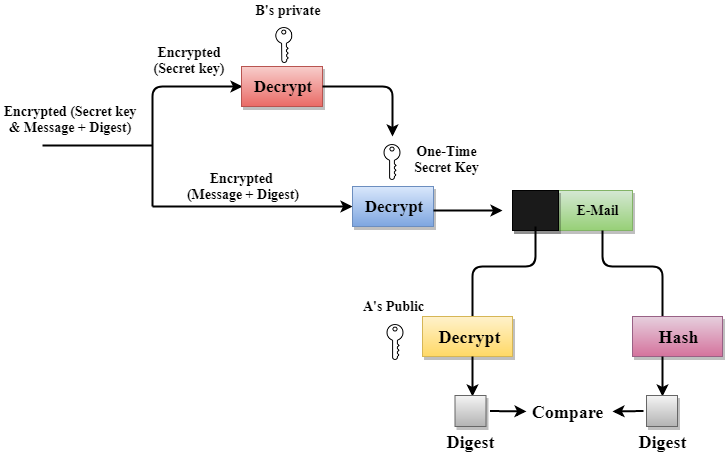
### PGP at the Sender site (A)



### Following are the steps taken to show how PGP uses hashing and a combination of three keys to generate the original message:

* The receiver receives the combination of encrypted secret key and message digest is received.
* The encrypted secret key is decrypted by using the sender's private key to get the one-time secret key.
* The secret key is then used to decrypt the combination of message and digest.
* The digest is decrypted by using the sender's public key, and the original message is hashed by using a hash function to create a digest.
* Both the digests are compared if both of them are equal means that all the aspects of security are preserved.

### PGP at the Receiver site (B)



### Disadvantages of PGP Encryption

* **The Administration is difficult:** The different versions of PGP complicate the administration.
* **Compatibility issues:** Both the sender and the receiver must have compatible versions of PGP. For example, if you encrypt an email by using PGP with one of the encryption technique, the receiver has a different version of PGP which cannot read the data.
* **Complexity:** PGP is a complex technique. Other security schemes use symmetric encryption that uses one key or asymmetric encryption that uses two different keys. PGP uses a hybrid approach that implements symmetric encryption with two keys. PGP is more complex, and it is less familiar than the traditional symmetric or asymmetric methods.
* **No Recovery:** Computer administrators face the problems of losing their passwords. In such situations, an administrator should use a special program to retrieve passwords. For example, a technician has physical access to a PC which can be used to retrieve a password. However, PGP does not offer such a special program for recovery; encryption methods are very strong so, it does not retrieve the forgotten passwords results in lost messages or lost files.