**Network Security Using Cryptography**

****

**Table of Contents**

[Introduction 4](#_Toc94610369)

[Network 4](#_Toc94610370)

[What is Network Security? 4](#_Toc94610371)

[Working of Network Security 5](#_Toc94610372)

[Physical Network Security 5](#_Toc94610373)

[Technical Network Security 6](#_Toc94610374)

[Administrative Network Security 6](#_Toc94610375)

[Types of Network Security 6](#_Toc94610376)

[• Network Access Control 6](#_Toc94610377)

[• Antivirus and Antimalware Software 7](#_Toc94610378)

[• Firewall Protection 7](#_Toc94610379)

[• Virtual Private network 7](#_Toc94610380)

[Types of Attacks in the Network 7](#_Toc94610381)

[Passive Attacks 7](#_Toc94610382)

[Active Attacks 8](#_Toc94610383)

[Need for Network Security 8](#_Toc94610384)

[• Data Security 9](#_Toc94610385)

[• Secure Communication 9](#_Toc94610386)

[• Prevents Cyber-threats 9](#_Toc94610387)

[• Safer Authentication 9](#_Toc94610388)

[• Access Control 10](#_Toc94610389)

[• Detecting System Failure 10](#_Toc94610390)

[Cryptography 10](#_Toc94610391)

[Working of Cryptography in Network Security 10](#_Toc94610392)

[Generation of Key Pairs 10](#_Toc94610393)

[Encryption 11](#_Toc94610394)

[• Substitution 11](#_Toc94610395)

[• Transposition 11](#_Toc94610396)

[Decryption 12](#_Toc94610397)

[Types of Cryptography 12](#_Toc94610398)

[Symmetric Cryptography 12](#_Toc94610399)

[Asymmetric Cryptography 13](#_Toc94610400)

[RSA 14](#_Toc94610401)

[DSA 15](#_Toc94610402)

[Diffie-Hellman Key Exchange 15](#_Toc94610403)

[ECDSA 16](#_Toc94610404)

[Hybrid Cryptography 16](#_Toc94610405)

[Hash Functions 16](#_Toc94610406)

[Features of Cryptography in Network Security 17](#_Toc94610407)

[• Non-modification of Data 18](#_Toc94610408)

[• Information Remains Protected in the Network 18](#_Toc94610409)

[• The Verified User Can Access the Network 18](#_Toc94610410)

[• The details of Data Transmitted and Received in the Network are Determined 18](#_Toc94610411)

[• The Control of the Resources Present in the Network is Obtained 18](#_Toc94610412)

[Benefits of Cryptography in Network Security 18](#_Toc94610413)

[Secure Authentication 18](#_Toc94610414)

[Secure Communication 18](#_Toc94610415)

[Increases Customer Satisfaction 19](#_Toc94610416)

[Data Security 19](#_Toc94610417)

[Secure Methodology 19](#_Toc94610418)

[Company Reputation and Growth 19](#_Toc94610419)

[Challenges of Cryptography in Network Security 20](#_Toc94610420)

[Cryptographic Key Compromise 20](#_Toc94610421)

[Conclusion 22](#_Toc94610422)

# **Introduction**

Network security plays an essential role in this digital world. All things are connected to a network to transmit and receive data securely. The network acts as a boom to an organization for better communication between the intended users. The issues arise as the third party intrudes into the network to disrupt or steal the data. An organization transfers critical information through the network, and hence the network is to be protected against unauthorized access. Cryptography uses secured techniques to send and receive data within the network. This article provides brief details about network security using cryptography.

# **Network**

The network comprises various components or devices like computers, routers, and other network devices to enable efficient communication or data sharing. The network plays a significant role in connecting devices from various locations worldwide. A common example of any network is the internet that connects all the users from different locations.



Figure 1: [A simple Network Consisting of a Computer, Server, Laptop, Mobile Phone, etc](https://ophtek.com/wp-content/uploads/2013/07/networking_540x405.jpg).

Networks can be the public or private type where the former allows its users to access all the resources in the network. The private network allows only authorized users to access the network's resources. It is used to share the data or resources among the network devices. It provides quicker communication between the users in the network. It allows multiple users to share hardware or software within the network to perform their functions.

Network structure varies depending upon the function it performs. The management of the network becomes more challenging as the network becomes complex. The network act as a common platform for components and the user connected to it. The threats and malware intruding in the system affect all the devices and the users present in the network.

# **What is Network Security?**

Network Security is the process of securing all resources present in the network. It involves policies, standards, and procedures involving hardware, software, and technology to secure the intended network components from unauthorized access. Each organization has a different network infrastructure for handling its functions. It follows a variety of network solutions depending on the requirements. It helps the organization protect itself from the arising cyber-threats in this digital world.



Figure 2: [Network Security](http://www.pro-v2u.com/managed-network-security/)

The motive of network security is to provide access to authorized users, which automatically prevents unauthorized users from entering the network and accessing critical organizational resources. Therefore, network security plays a prominent role in the organization. It clears the traffic prevailing in the network to provide efficient functioning of the organization. It also detects abnormalities in the network and notifies the administrator. The protective measures will strengthen the security of the organizational network.

# **Working of Network Security**

Cyber threats arise in various layers in the infrastructure of the organization. The network layer addresses the issues and enhances the organization's security. Hardware, software, and policies are designed to manage the secure functioning of physical, technical, and administrative controls in network security.

A picture containing graphical user interface

Description automatically generated

<https://purplesec.us/security-controls/>

## **Physical Network Security**

Physical Network Security plays a significant role in safeguarding the data, servers, and networks. However, the exploitation of the physical devices causes a severe impact on the organization. Though the physical devices cover the insurance policies to recover from such disasters, the effects would interrupt the organization's growth. Therefore, the organization should protect its devices from theft, natural disasters, and accidents. Therefore, the proper maintenance and security of the physical device will enhance the organization's functioning.

## **Technical Network Security**

Technical Network Security aims to protect the data from cyber-attacks and threats from the insiders. Data security is achieved by encrypting the information transmitted over the network. A third party cannot alter or view the information and provides enhanced data security. It helps to protect the personal and confidential information of the organization. Thus, it enhances customer trust and increases the reputation of the organization.

## **Administrative Network Security**

Administrative Network Security compresses standards and policies to implement network security across the organization. It includes authorization and access control to allow legitimate users to access the critical organization's infrastructure. In addition, it helps to identify unauthorized access and detect the threats entering the network. Thus, it helps in enhancing the data security of the organization.

# **Types of Network Security**

Network Security comes in different forms over the organization's security. Some of the notable ways to enhance the security of the organization include,

* **Network Access Control**

Network Access control secures confidential data and resources by granting access to legitimate users. The user's access to the network is provided as per the requirements. Therefore, it helps to avoid leakage of data due to human error. Furthermore, it avoids the unauthorized access of the resources to the sensitive resources of the organization.

* **Antivirus and Antimalware Software**

Antivirus and Antimalware Software plays a significant role in the organization's security. It detects the threats, malware, and other threats that affect the organization and reject it from the network. As a result, it increases the network security of the organization.

* **Firewall Protection**

A firewall acts as a protective shield between the organization and other users entering the organization's network. It sets regulations of the connections entering the network. The Firewall rejects the access of the users other than the prescribed standards. Thus, it protects the organizational network from malware, viruses, and spyware.

* **Virtual Private network**

A virtual private network is created between the organization and a user at a different location. It is used to provide secure encrypted communication between the two nodes. It enhances data security and secures the transmission from threats.

# **Types of Attacks in the Network**

The network is the common medium for different vectors, responsible for transferring resources. Therefore, it is an area of interest for cyber-attackers to control network systems. The network attacks are of two types: active attacks and passive attacks.

## **Passive Attacks**

Passive attacks are a form of attack undertaken by the hacker to obtain the details about the network. It includes reading the message content and analysing the traffic of the network. It is usually done without the knowledge of the network administrator.



Figure 4: [Passive Attack](https://techdifferences.com/difference-between-active-and-passive-attacks.html)



Figure 5: [Active Attack](https://techdifferences.com/difference-between-active-and-passive-attacks.html)

## **Active Attacks**

Active attacks are performed to alter the message transmitted through the network. The fake messages or mail containing the malware is introduced in the network to disrupt the normal work function. The active attacks are as follows.

* Modification of the message of the sender.
* Denial of Service to critical resources.
* Exploiting the network functions.

# **Need for Network Security**

An organization needs to maintain its working functionalities. The motive behind securing the network is to protect all the resources from vulnerabilities available in the network. The network security ensures that all the data, files, and components are protected from external and internal threats.

* **Data Security**

Data Security plays a key role in the successful functioning of any organization. Data breaches cause severe damage to the organization’s work function and its reputation. The network security handles all the data more securely to protect it against internal and external threats.

* **Secure Communication**

Network security provides secure communication between the users. It encrypts the message transmitted over the network to avoid the third party from viewing the information. The different encryption techniques are employed as per the requirement to deliver secure communication.

* **Prevents Cyber-threats**

It monitors the functions that take place in the network. The abnormalities in the normal function of the network are detected and are notified to the network administration. It detects the malware and prevents them from entering the network. The data transmitted over the network are encrypted, and access is denied viewing the message in the network.

* **Safer Authentication**

Authentication is the process of verifying the identity of the user. It ensures that unauthorized access is denied at the doorway. The user is verified before entering the network. The secure authentication methodology is followed to achieve efficient authentication.

* **Access Control**

The authorized users are only allowed to access all the critical resources of the network. The other users can access only the allocated resources. Thus, network security provides access control to avoid critical data exposure outside the network.

* **Detecting System Failure**

The network security identifies the error in the functioning of the network components. It detects the system failures and notifies the system administrator to rectify the damage. It also backups the data in the network to function effectively during system failures.

**Cryptography**

Cryptography is the art of securing all the transactions over the network that ensures secure communication, file transfers, authentication processes, etc. The organization follows this technique to deliver the protected network to its users to prevent cyber-attacks. Unfortunately, the non-protected network attracts unauthorized users to capture the data resources and interrupt the functions of the network.

Cryptography uses the mathematical concept to create an algorithm to deliver a secure communication strategy. The algorithm converts the sender's message into a non-readable cipher text. It can only be converted into the original text by the receiver. Thus, it maintains data security and enhances data privacy. Furthermore, it achieves the integrity, confidentiality, non-repudiation, and authenticity of the data in the network.

# **Working of Cryptography in Network Security**

Cryptography delivers its secure functioning through the process called encryption and decryption. Encryption refers to transforming the original message into ciphertext using a specific algorithm. The encrypted text is hard to be recovered without the decryption keys. On the other hand, decryption converts the ciphertext into a readable original message. Cryptography techniques use pairs of keys to undertake the process of encryption and decryption.

## **Generation of Key Pairs**

Cryptography uses secure key pairs to provide complete protection during authentication and communication. These keys are the public and private keys that can be generated manually by the system administrator or automatically by the Automated Certificate Management System.

These cryptographic key pairs are used to provide access to the critical structures of the organization. The private key generated by the system is kept secure and never transmitted over the network. The public key is authenticated and validated to bring it into access. A certificate authority (CA) authorizes the public key and is bound to a fully qualified domain name. The authorized public key becomes an x509 certificate. The organization uses the generated keys to provide secure access and communication. Automated Certificate Management System is used to issue and manage certificates across devices and services. It reduces the risk of service outage and access denial due to expired and invalid certificates.

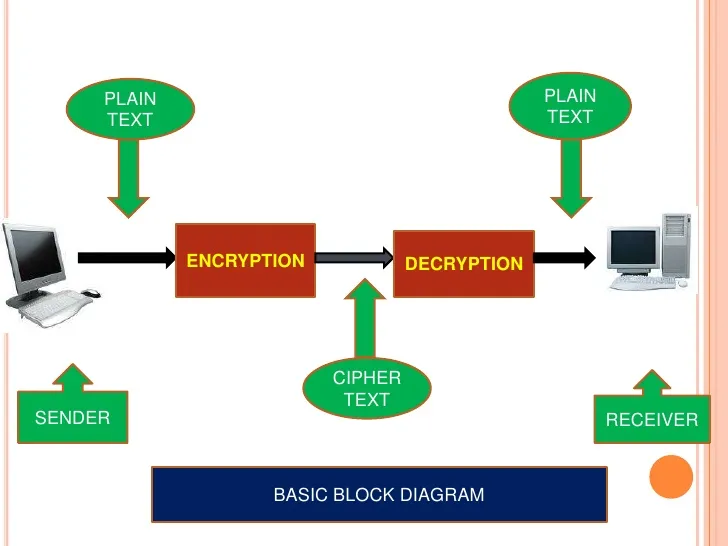


Figure 7: [Working of Cryptography in Network Security](https://www.thecrazyprogrammer.com/2019/07/types-of-cryptography.html)

## **Encryption**

Plaintext refers to all sorts of information transmitted by the sender. The user can transmit information like personal information, company resources, confidential files, etc., in a network. Attackers can benefit from the data when the original text is transmitted over the network. Therefore, the original text is changed into a non-readable format using a key to remain protected in the network. This process is called encryption.

Encryption works on two principles:

### **Substitution**

Substitution is the process of mapping the original plaintext into ciphertext. The algorithm converts each letter in the original message into a relevant symbol or letter. A simple example is given below.

The original message is ABCDE, and the key given for the encryption process is OPQ. Hence, the key will produce the substitution alphabet for the plain text as

|  |  |
| --- | --- |
| PLAIN TEXT ALPHABET | ABCDEFGHIJKLMNOPQRSTUVWXYZ |
| SUBSTITUTION ALPHABET: | OPQABCDEFGHIJKLMNRSTUVWXYZ |

The encrypted message for the ABCDE is OPQAB.

### **Transposition**

A cryptography encryption process that converts the original message into the ciphertext by the permutation process is called transposition.

A simple encryption example is as follows.

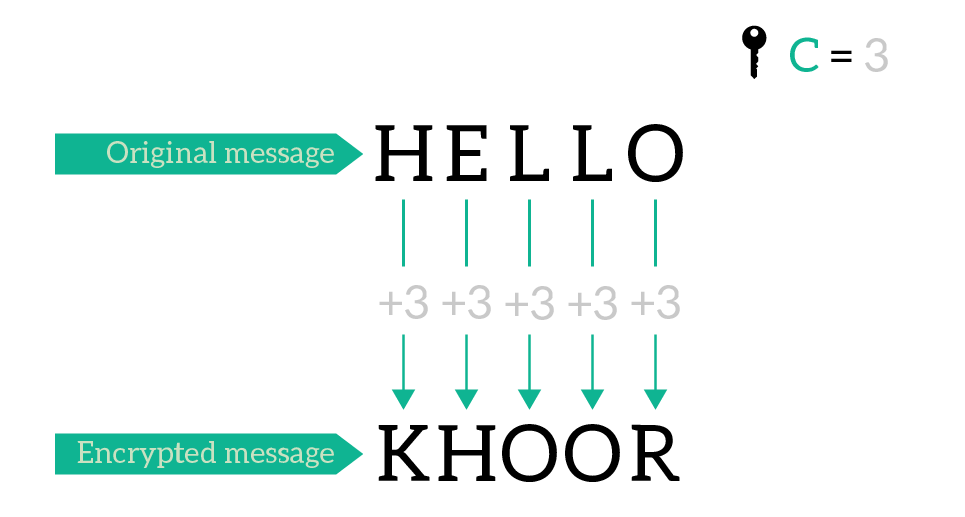


Figure 8: [Example for Transposition Encryption](https://www.ictshore.com/network-security/what-is-encryption/)

Consider the original message as HELLO and the given key is C taken as number 3. The encrypted message is obtained by adding three to each letter in the original message. It becomes H to K, E to H, L to O, L to O, and O to R. The encrypted ciphertext is KHOOR.

Both substitution and transposition techniques are used in different applications.

Encryption delivers adequate security to data travelling in the network. It ensures that the intended user can view the original transmitted text with the specific key. Thus, the intended data is protected, and the exposure is rejected. Furthermore, if the attacker compromises the system, the captured data remains encrypted.

## **Decryption**

Decryption means recovering the initially transmitted message from the ciphertext and delivering it to the user. The decryption process is the reverse process of encryption. The decryption can be done only by the key allocated during the encryption process. The decryption key should be kept private to maintain the protection of the data. If the decryption key is made public, users with the decryption key can recover the message and benefit themselves. The encrypted message in the medium is decrypted and made available for the receiver to view the content. The encrypted message recovered by the attacker cannot extract the data without the decryption key. Hence, the process of decryption maintains the integrity of the message.

# **Types of Cryptography**

Cryptography is the technique of securing communication over the unsecured channel. Cryptography is of three types, namely,

* Symmetric cryptography
* Asymmetric cryptography
* Hybrid cryptography
* Hash Functions

## **Symmetric Cryptography**

An encryption process that uses the same key for both encryption and decryption of messages transmitted over the network is called symmetric cryptography.

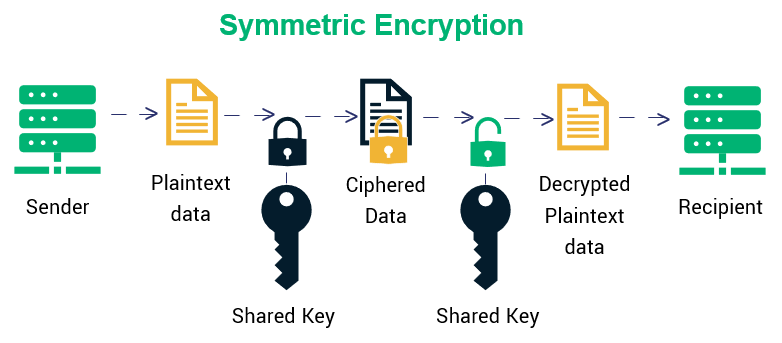


Figure 9: [Symmetric Cryptography](https://sectigostore.com/blog/types-of-encryption-what-to-know-about-symmetric-vs-asymmetric-encryption/)

The message from the sender is converted into a non-readable ciphertext using a specific key, and it is transmitted over the network. The same key decrypts the non-readable ciphertext into the original message format. The sender and receiver share the common key for encryption and decryption. The shared key is placed securely to avoid the cyber-threats. This kind of encryption is widely used to encrypt large amounts of data.

## **Asymmetric Cryptography**

The secure work function provided by cryptography is also achieved through asymmetric encryption. Asymmetric encryption uses different keys to decrypt the connections for secured communication. This form of encryption process is also called public-key encryption.

It uses a mathematically derived pair of keys known as a public key and a private key. The user with the desired private key gains accesses to the system with the public key. The public key is used to encrypt the data for secure communication. The private key decrypts the encrypted data to obtain the original content when the receiver opens the document. The public and private keys are mathematically related, but the latter cannot be derived from the former.

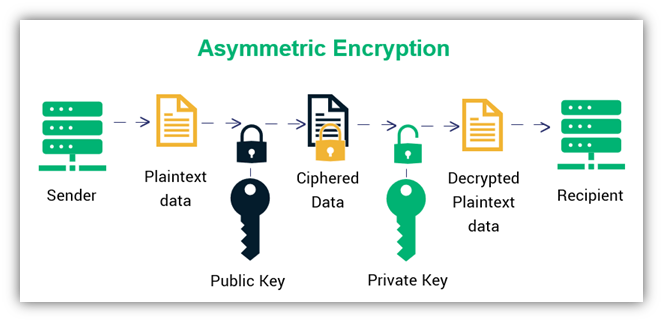


Figure 10: [Asymmetric Encryption](https://sectigostore.com/blog/types-of-encryption-what-to-know-about-symmetric-vs-asymmetric-encryption/)

The organization can use asymmetric encryption for a secure authentication process to allow or deny access to its users.

Diagram

Description automatically generated

Figure 11: [Asymmetric Encryption for Authentication](https://sectigo.com/resource-library/what-is-an-ssh-key)

The authentication process is initiated when the user requests the remote server. Upon getting the request from a client to grant access to the user, the server gives a challenge request to the user. The challenge request is encrypted using the shared public key, and it is sent to the client. The user should correctly solve the challenge request to access the system. The private key decrypts the response to the request and sends it to the server. The server grants access if the decrypted request is correct. The server automatically initiates the challenge request to the client, and no manual process is involved.

The asymmetric algorithm used for key exchange and digital signature includes

* RSA
* DSA
* Diffie-Hellman key exchange
* ECDSA

### **RSA**

RSA (Rivest-Shamir-Adleman) is the oldest public-key cryptosystem. It is generally used to transmit data securely. The key is the product of two large prime numbers whose digital length is more than 100. It is a slow algorithm since no relevant techniques are used to solve the large keys. Nevertheless, it is commonly used for bulk encryption and decryption. There is the possibility of breaking these prime algorithms in the future.

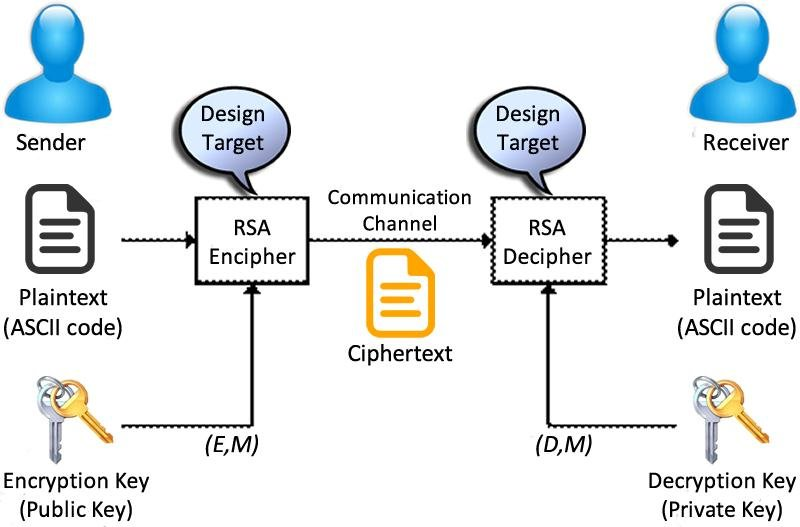


Figure 12: [Working of RSA Algorithm](https://www.researchgate.net/figure/RSA-algorithm-structure_fig2_298298027)

### **DSA**

DSA is a Digital Signature Algorithm used to verify the message's origin, sender, and genuine nature. DSA generate and verify the digital certificate by employing modular exponentiation and discrete logarithm problem. The public and private keys are generated using a complex mathematical process. The private key develops the digital certificate using the given message and it is verified by the public key. It ensures the receiver that the received message is from a trusted source. It is used to authenticate messages, verify the originality of the message, and detect spam messages.

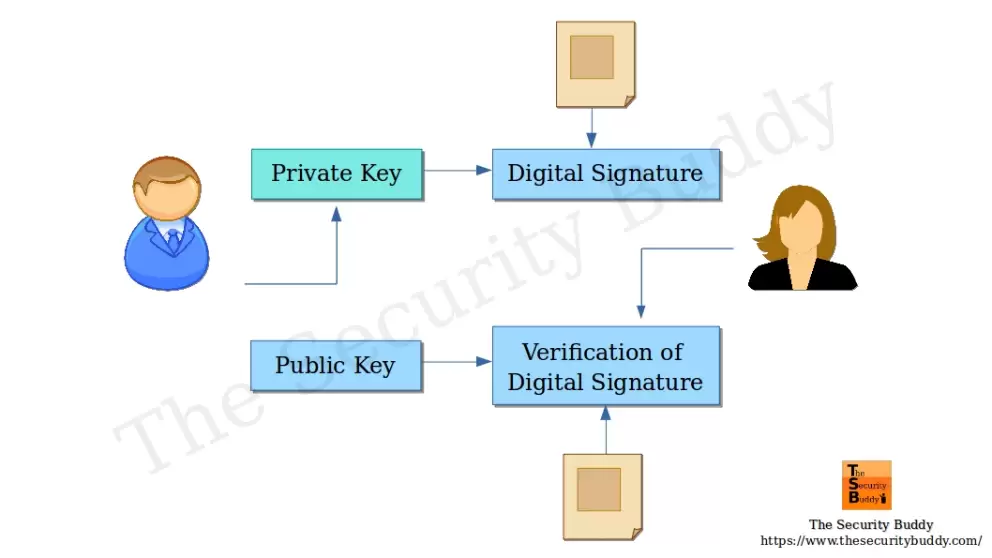


Figure 13: [Working of DSA Algorithm](https://www.thesecuritybuddy.com/encryption/how-does-digital-signature-algorithm-dsa-work/)

### **Diffie-Hellman Key Exchange**

The Diffie-Hellman Key Exchange algorithm shares the cryptographic key between the two users for secure communication. This algorithm is used for only key exchange to deliver secure communication over the unsecured channel. In addition, it helps the users to share the cryptographic key more safely. This method of exchange is not used for authentication or digital signature.

### **ECDSA**

ECDSA (Elliptic Curve Digital Signature Algorithm) is a new Digital Signature Algorithm that uses elliptic curves to enforce an encryption process. This method is known as elliptic curve cryptography. It provides a high level of security with a shorter key length. Most SSH clients use the ECDSA algorithm in current system applications.

## **Hybrid Cryptography**

The advantage of both symmetric and asymmetric encryption brings out hybrid cryptography. Hybrid cryptography enhances the network's security by imposing the techniques of both cryptographies. First, symmetric cryptography is used to encrypt the sender's original message using the key. Then, the key is encrypted using asymmetric cryptography. Next, the encrypted message and the encrypted key are transmitted over the network. Next, the receiver decrypts the symmetric key using the private key. Finally, the original message is obtained from the symmetric key.

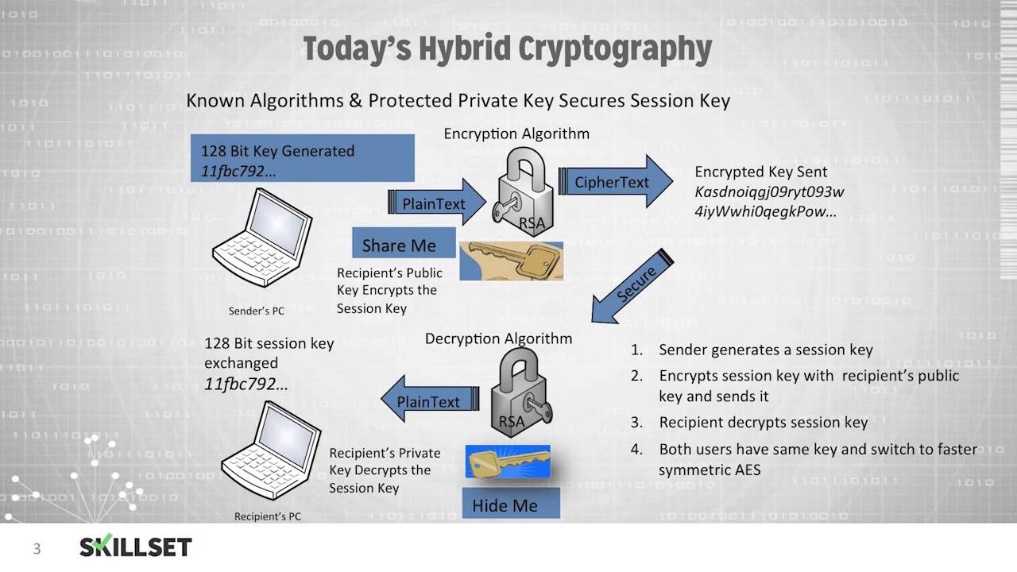


Figure 14: [Hybrid cryptography](https://www.youtube.com/watch?v=VPvZbMXfv_0)

The cryptography method creates a secure communication channel between the sender and the receiver. Moreover, the double encryption in the communication will enhance the safety feature. Hence, it provides a protective method of data transfer in the network.

## **Hash Functions**

Hash Functions are algorithms that use no keys to undertake the encryption process. It is referred to as one-way encryption. A hash function is a message digest that acts as a unique identifier for the original message. The original message from the sender is processed using the mathematical algorithm to produce an unreadable hash output. It is a one-way source. The converted message file cannot be recovered using any algorithm. It delivers the message to the receiver the same way it is transmitted. Each text will generate a different hash value. This condition makes it impossible for hackers to crack it using the brute force technique.

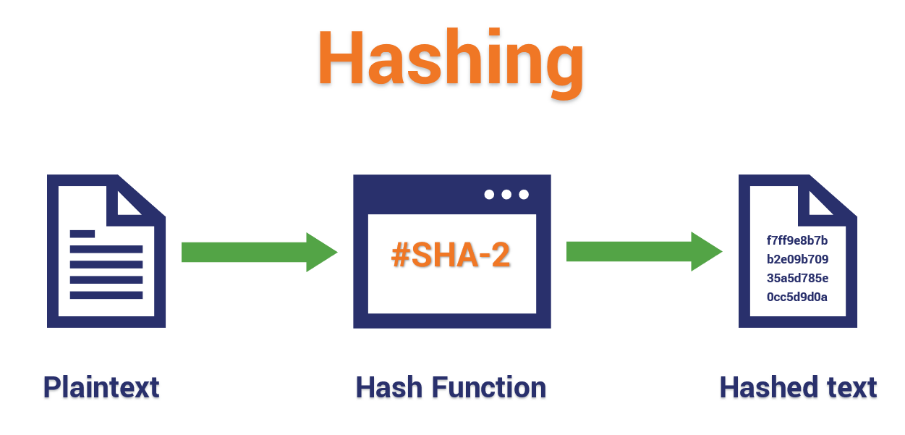


Figure 15: [Hashing Function](https://www.thesslstore.com/blog/what-is-a-hash-function-in-cryptography-a-beginners-guide/)

Hash Functions are commonly used to secure passwords. It is also used to maintain the integrity of the data in the network. In addition, it is used by the organization for a safer authentication process and efficiently organizing files.

# **Features of Cryptography in Network Security**

The security tools use various techniques and procedures to secure the information and devices in the network. The efficiency of these tools and techniques relies on how well the data is securely transmitted over the network. The information describing the genuineness of the data is essential in maintaining data security through the network. The quality of data processed before transmission and recovery of the transmitted data to the receiver is essential. Hence, the features of network security are the following.

Figure 16: Features of Cryptography in Network Security

## **Non-modification of Data**

Data integrity refers to securing the information created by the sender in the network. First, the data is encrypted to transmit securely over the network. Then, the encrypted data is decrypted to deliver the original information to the receiver. Finally, the original data is recovered and viewed by the receiver. This feature assures its users that the receiver receives the transmitted data.

## **Information Remains Protected in the Network**

Confidentiality refers to securing the information exposed or accessible to unauthorized parties. The user with the intended access is only allowed to view or process the data. It maintains the network’s information privacy to prevent network users from viewing the transmitted content. It confirms that the transmitted message remains useless when an unauthorized party intrudes or attacks the organizational system.

## **The Verified User Can Access the Network**

Multiple connected components in the network may have critical information or data resources. The cyber-attacker or unauthorized user can access the resources in the network. There are chances of altering the data or copying the content to expose it on the public web without the network administrator's knowledge. The authentication employed in the network allows access to the desired individual to maintain the secure functioning of the processes in the network.

## **The details of Data Transmitted and Received in the Network are Determined.**

The network security gives non-repudiation of the message. It refers that the receiver can obtain the details of the transmitted message to ensure that the received information is valid. The sender can also acknowledge the details about the transmitted message received by the receiver. Therefore, both parties cannot deny their charge in the time of emergency. It also helps the receiver to detect and eliminate messages from unauthorized users. On the other hand, the sender can ensure the data is received, which helps identify the error during the transmission.

## **The Control of the Resources Present in the Network is obtained**

Access control provides limited access to the authorized individual to gain connections with the resources in the network. It identifies and rejects unauthorized persons from entering the network. The person can access only the authorized resources, and other resources are accessed via proper permission. It helps to prevent the leakage of critical resources to the outside world.

# **Benefits of Cryptography in Network Security**

## **Secure Authentication**

* The cryptographic methodology provides authentication credits.
* Cryptography uses pair of keys to encrypt and decrypt the messages. Therefore, it is considered a better choice of authentication than the traditional login process using usernames and passwords.

## **Secure Communication**

* The encryption and decryption of messages provide better security to the message transmitted over the network. It is embedded in the systems to encrypt and decrypt data automatically. Thus, it helps the user securely transit their private information like personal details, account details, and confidential information.
* In addition, it ensures that the information is unreadable by the third party in the transmission medium.

## **Increases Customer Satisfaction**

* Cryptographic techniques are used to safeguard user information and secure itself from huge penalties.
* Network security protects the user's private information by encrypting it before transmitting it over the network.
* Cryptography techniques are employed to gain customers' trust by protecting their information from cyber threats.

## **Data Security**

* The cryptographic methodology allows only the intended user to access the resources in the network. Furthermore, the identity of the users entering the system is verified. Thus, it prevents unauthorized third parties from accessing the network.
* The messages cannot be altered or changed during the transmission over the channel. It maintains the genuine nature of the information and delivers it to the receiver.
* The details of the message are transmitted along with the ciphertext. Therefore, the receiver can verify whether the data is from trusted resources.

## **Secure Methodology**

* The keys used in the cryptographic technique are created mathematically, and it is hard to crack the formula. The Public key is used to encrypt the process, and a private key is used to decrypt the process. It acts as a secure tool for communication.

## **Company Reputation and Growth**

* The security features of cryptography protect the user's information from data breaches. In addition, it increases the company's reputation.
* The increase in organizational reputation and customer trust enhances the organization's growth.

Diagram

Description automatically generated

Figure 17: [Benefits of Cryptography in Network Security](https://www.techtarget.com/searchsecurity/definition/cryptography)

# **Challenges of Cryptography in Network Security**

Organizations widely use cryptographic techniques to create a secure working environment. However, it poses some challenges in the network security as follows.

* The network administrator cannot gain complete control over the data transmission as they are encrypted. Hence, the profile of the message cannot be monitored when transmitted over the network.
* It cannot detect the documents transferred beyond the network when cyber-criminals compromise the employee.
* If the decryption key is lost, there is no way to recover the original text. Hence, the message remains encrypted.
* The earlier encryption process is cracked by brute force to guess the possible combination and decrypt the ciphertext.
* Managing a complex network is a challenging and tedious process because human error causes severe damage to the organization.
* The standard and certification could expire, causing a denial of access to the critical resources. The periodic renewal is necessary to maintain a continuous workflow.
* The cryptographic algorithm may reject the legitimate users' connectivity whose accounts are incompatible with the standards.
* It does not guard the network against poor system maintenance. Thus, it is a weak line for the attack to cyber-criminals to enter the organization.
* The cryptographic methodology installation and maintenance costs are high to the organization.
* Cryptographic techniques are used only to encrypt and decrypt the text. The organization should invest in other security tools to protect itself from other incoming threats.

## **Cryptographic Key Compromise**

The cryptographic key acts as a gateway to the critical organization infrastructure. Since the management of the keys is essential to obtain a safe working environment. The loss or mismanaged keys may cause severe effects on the organization.

If the hacker obtains the lost key, the following things are possible.

* It may lead to unauthorized access of the system resources that lead to the disclosure of sensitive information.
* The unauthorized party may introduce malware to disrupt the entire functionalities of the organization.
* It may lead to email compromise to transfer the funds and data to the hacker.
* A single key may help the hacker gain access to other intended resources of the organization.
* The disclosure of sensitive information due to the loss of the SSH key may lead to loss of the business reputation.
* The exposure of the customer data leads to a loss of trust among its users.
* A huge fine is paid against the personal data exposure of its users.
* The loss of the key may restrict entry to the critical data resources developing error messages.
* The key mismanagement may provide access to critical resources leading to compromise of the organizational resources and exploiting the company’s functions.

The cryptographic key is generated, identified, verified, and approved to work in the network. The encryption and decryption should be done quickly to deliver an efficient process. Cryptographic key management is a tedious process when done manually. These processes are to be automated to obtain an efficient workflow.

# **Conclusion**

Cryptography is an emerging technology that is used for secure data communication. Network security using cryptography has provided eminent security to the information transferred through the network. The attacker who unauthorizedly enters the network cannot read the transferred data as it is encrypted. The information transmitted in the network can be decrypted only by the intended receiver. Therefore, the intended user and receiver can securely communicate in the network. The techniques used for the encryption and decryption process are easy to deploy and hard to crack by the attackers. The different methodology related to cryptography is employed for a different purpose to secure the organization's critical resources.