What is Data Encryption?

Last Updated : 02 Jan, 2025

Data encryption is the process of converting readable information (plaintext) into an unreadable format (ciphertext) to protect it from unauthorized access. It is a method of preserving data confidentiality by transforming it into ciphertext, which can only be decoded using a unique decryption key produced at the time of the encryption or before it. The conversion of plaintext into ciphertext is known as encryption. By using encryption keys and mathematical algorithms, the data is scrambled so that anyone intercepting it without the proper key cannot understand the contents.

When the intended recipient receives the encrypted data, they use the matching decryption key to return it to its original, readable form. This approach ensures that sensitive information such as personal details, financial data, or confidential communications remains secure as it travels over networks or is stored on devices.

Key Objective of Encryption Data

- **Confidentiality:** Encryption ensures that only authorized parties can get access to data and recognize the information.
- **Data Integrity:** Encryption can also provide data integrity by making sure that the encrypted data remains unchanged during transmission. Any unauthorized changes to the encrypted information will render it undecipherable or will fail integrity checks.

- **Authentication:** Encryption may be used as part of authentication mechanisms to verify the identification of the communication party.
- **Non-Repudiation:** Through encryption, events can make sure that they cannot deny their involvement in growing or sending a selected piece of data.

Importance of Data Encryption

The significance of encryption cannot be overstated in any way. Even though your data is stored in a standard infrastructure, it is still possible for it to be hacked. There's always the chance that data will be compromised, but with data encryption, your information will be much more secure. Consider it this way for a moment. If your data is stored in a secure system, encrypting it before sending it out will keep it safe. Sanctioned systems do not provide the same level of protection.

So, how do you think this would play out in real life?

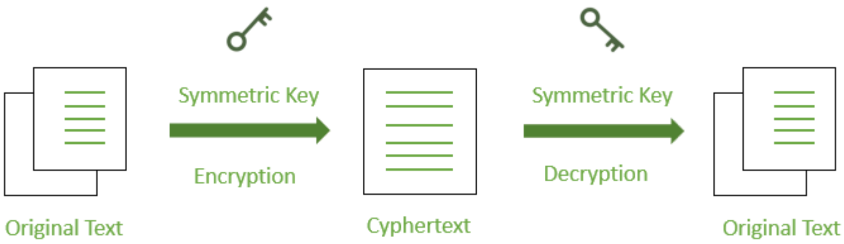
Suppose the user has access to sensitive information while at work. The user may put the information on a portable disc and move it anywhere they choose without any encryption. If the encryptions are set in place ahead of time, the user can still copy the information, but the data will be unintelligible when they try to see it somewhere else. These are the benefits of data encryption that demonstrate its genuine value.

Types of Data Encryption

There are multiple encryption techniques, each of which have been developed with various security requirements in mind. Symmetric and Asymmetric encryption are the two types of data encryption.

1. Symmetric Key Encryption

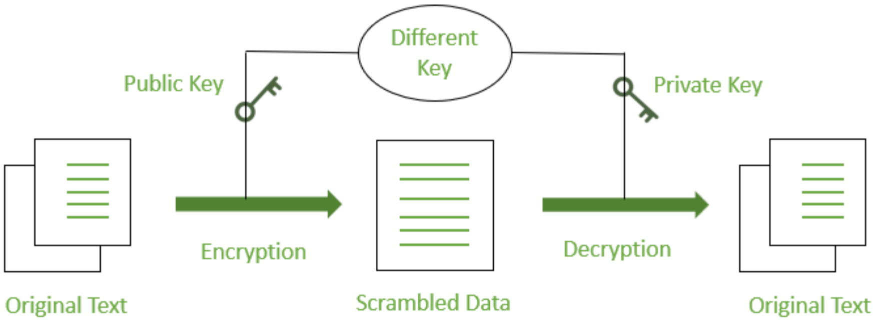
There are a few strategies used in cryptography algorithms. For encryption and decryption processes, some algorithms employ a unique key. In such operations, the unique key must be secured since the system or person who knows the key has complete authentication to decode the message for reading. This approach is known as “symmetric encryption” in the field of network encryption.



Symmetric Encryption

2. Asymmetric Key Encryption

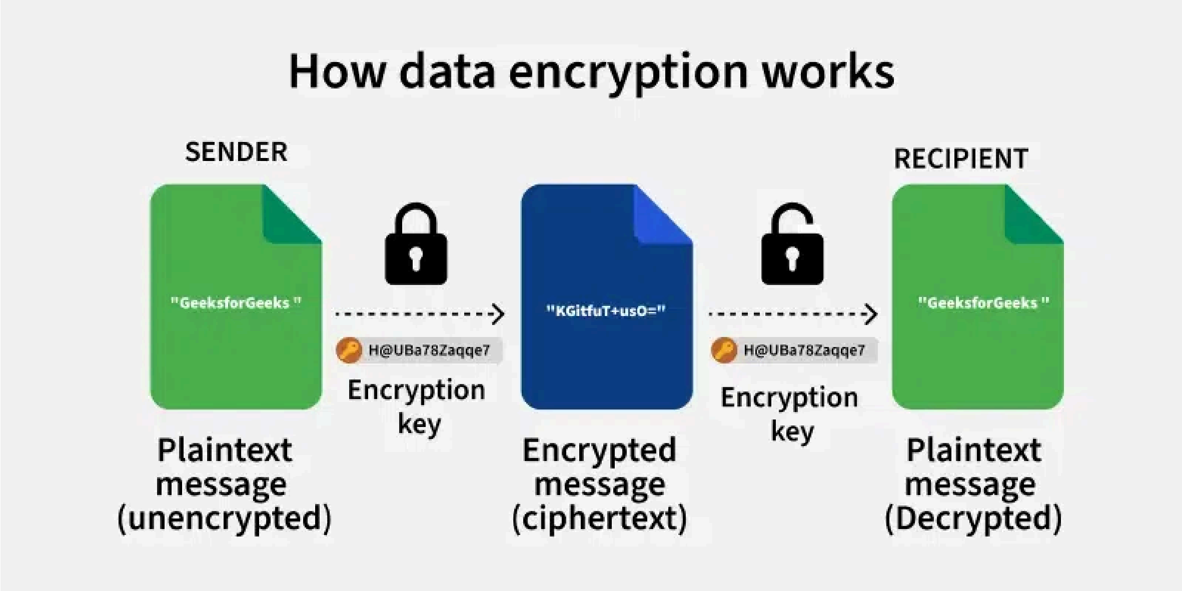
Some cryptography methods employ one key for data encryption and another key for data decryption. As a result, anyone who has access to such a public communication will be unable to decode or read it. This type of cryptography, known as “public-key” encryption, is used in the majority of internet security protocols. The term “asymmetric encryption” is used to describe this type of encryption.



Asymmetric Encryption

How Does Encryption Work?

When data or information is shared over internet, it passes via a number of global network devices that are a component of the public internet. Data that is transmitted via the open internet leads to the risk of being stolen or hacked by hackers. Users can install particular hardware or software to guarantee the safe transfer of data or information in order to avoid hacking. In network security these operations are referred to as encryption. The process of transforming plaintext into ciphertext, is called encryption.


How data encryption works
SENDER
RECIPIENT
"GeeksforGeeks "
H@UBa78Zaqqe7
Encryption key
"KGitfuT+usO="
H@UBa78Zaqqe7
Encryption key
"GeeksforGeeks "
Plaintext message (unencrypted)
Encrypted message (ciphertext)
Plaintext message (Decrypted)

Working of Encryption

On the left you have an original, readable message called plaintext such as “**GeeksforGeeks**.” Before sending it over a network, the sender uses an encryption key and an encryption process to convert this readable message into a scrambled, unreadable format known as ciphertext (in this image it is like “KGifuT+us0=”). This ciphertext travels across the internet, so if someone intercepts it, they cannot understand it without the key. When the ciphertext reaches the intended recipient, they use the matching decryption key and a decryption process to turn the unreadable ciphertext back into the original, readable message “**GeeksforGeeks**.” Essentially the image shows how encryption and decryption ensure that only authorized parties with the correct keys can access the information in its original form.

States of Data Encryption

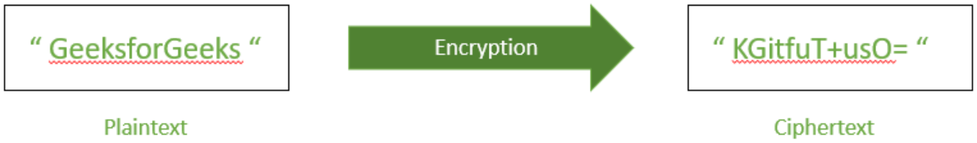
Data encryption in transit: Information that is actively moving from one point to another, such as via the internet or over a private network, is referred to as data in transit. Data is deemed less safe when in transit due to the weaknesses of transfer techniques.

Encryption of data at rest: Data encryption at rest decreases the risk of data breach caused by lost or stolen devices, inadvertent password sharing, or accidental permission granting by increasing the time it takes to access information and providing the time required to discover data loss, ransomware attacks, remotely erased data, or changed credentials.

How the Data Encryption Takes Place?

Data encryption transforms readable data known as plaintext, into an unreadable format called ciphertext. This process generally involves an algorithm and a unique encryption key. The algorithm uses the key to scramble the data in such a way that anyone without the key cannot make sense of the ciphertext.

When the intended recipient receives the encrypted data, they use the corresponding decryption key often related to the encryption key to reverse the process and restore the data to its original readable form. This approach ensures that even if someone intercepts the data during transmission they cannot understand it unless they have the correct key.



Encryption Process

Encryption is performed on digital communications, this technological procedure is designed to prevent a third party from deciphering the signal's secret content. Consumers conduct transactions for goods purchases over the internet. There are millions of web services that can help various trained employees do their responsibilities. Furthermore, to utilize these services that demand personal information, most websites require substantial identification. One of the most common ways, known as “encryption,” is to keep such information safe and secure.

Uses of Data Encryption

- Using digital signatures, Encryption is used to prove the integrity and authenticity of the information. Digital-rights management and copy protection both require encryption.
- Encryption can be used to erase data. But since data recovery tools can sometimes recover deleted data, if you encrypt the data first and then throw away the key, the only thing anyone can recover is the ciphertext, not the original data.
- Data Migration is used when transferring data over a network to ensure that no one else on the network can read it.
- VPNs (Virtual Private Networks) uses encryption, and you should encrypt everything you store in the cloud. This can encrypt the entire hard drive as well as voice calls.

Advantages of Data Encryption

- Data encryption keeps information distinct from the security of the device on which it is stored. Encryption provides security by allowing administrators to store and send data via insecure channels.
- If the password or key is lost, the user will be unable to open the encrypted file. Using simpler keys in data encryption, on the other hand, makes the data insecure, and anybody may access it at any time.
- Encryption improves the security of our information.

Disadvantages of Data Encryption

- If the password or key is lost, the user will be unable to open the encrypted file. Using simpler keys in data encryption, on the other hand, makes the data insecure, and anybody may access it at any time.
- Data encryption is a valuable data security approach that necessitates a lot of resources, such as data processing, time consumption, and the

use of numerous encryption and decryption algorithms. As a result, it is a somewhat costly approach.

- Data protection solutions might be difficult to utilize when the user layers them for contemporary systems and applications. This might have a negative influence on the device's normal operations.
- If a company fails to realize any of the restrictions imposed by encryption techniques, it is possible to set arbitrary expectations and

Data Encryption Algorithms

Depending on the use case, there are a variety of data encryption algorithms to choose from, but the following are the most commonly used:

- **DES (Data Encryption Standard)** is an old symmetric encryption algorithm that is no longer considered suitable for modern applications. As a result, DES has been superseded by other encryption algorithms.
- **Triple DES (3DES or TDES)**: Encrypts, decrypts, and encrypts again to create a longer key length by running the DES algorithm three times. It may be run with a single key, two keys, or three separate keys to increase security. 3DES is vulnerable to attacks such as block collisions since it uses a block cipher.
- **RSA** is a one-way asymmetric encryption algorithm that was one of the first public-key algorithms. Because of its long key length, RSA is popular and widely used on the Internet. It is used by browsers to create secure connections over insecure networks and is part of many security protocols such as SSH, OpenPGP, S/MIME, and SSL/TLS.
- **Twofish** is one of the fastest algorithms, with sizes of 128, 196, and 256 bits and a complex key structure for added security. It is available for free and is included in some of the best free software, including VeraCrypt, PeaZip, and KeePass, as well as the OpenPGP standard.
- **Elliptic Curve Cryptography (ECC)** was created as an upgrade to RSA and offers better security with significantly shorter key lengths. In the SSL/TLS protocol, ECC is an asymmetric method.

- **The** Advanced Encryption Standard (AES) is the encryption standard used by the US government. The AES algorithm is a symmetric-key algorithm that employs block cipher methods. It comes in sizes of 128, 192, and 256 bits, with the number of rounds of encryption increasing as the size increases. It was designed to be simple to implement in both hardware and software.

Conclusion

Encryption is a way of turning readable data into a secret code so that only authorized people can access it. It protects important information whether it’s being sent from one place to another or stored on a device from being seen by anyone who doesn’t have the right key to unlock it.

As we share and store more personal, financial, and business data online, encryption becomes more important. It helps keep our information safe, builds trust, and supports secure communication around the world.

Frequently Asked Question on Data Encryption

What happens when data is not encrypted?

It leads to Data Tampering. Encryption preserves the integrity of your emails in addition to their confidentiality. Emails are vulnerable to manipulation during transit if they are not encrypted.

How safe is it to use encryption?

The information that is encrypted cannot be read or processed until it has been decrypted. The basic building element of Data security is encryption.

Is data encryption unbreakable?