**Data Encryption**

Data Encryption 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 prior to it.

Data encryption converts data into a different form (code) that can only be accessed by people who have a secret key (formally known as a decryption key) or password. Data that has not been encrypted is referred to as plaintext, and data that has been encrypted is referred to as ciphertext. Encryption is one of the most widely used and successful data protection technologies in today’s corporate world.

Encryption is a critical tool for maintaining data integrity, and its importance cannot be overstated. Almost everything on the internet has been encrypted at some point.

**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.

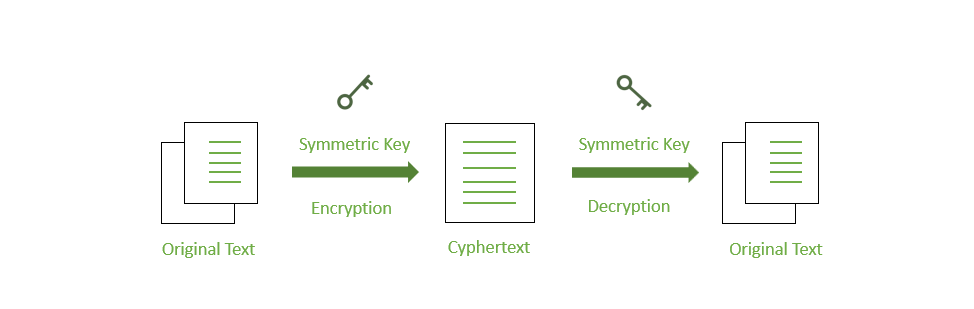
So, how do you think this would play out in real life? Consider the case of a user of a company’s data who has access to sensitive information while at work. The user may put the information on a portable disc and move it anywhere they choose without any encryption. If the encryptions are set in place ahead of time, the user can still copy the information, but the data will be unintelligible when they try to see it someplace else. These are the benefits of data encryption that demonstrate its genuine value.

**Types of Data Encryption:**

1. Symmetric Encryption
2. Asymmetric Encryption

 Encryption is frequently used in one of two ways i.e. with a symmetric key or with an asymmetric key.

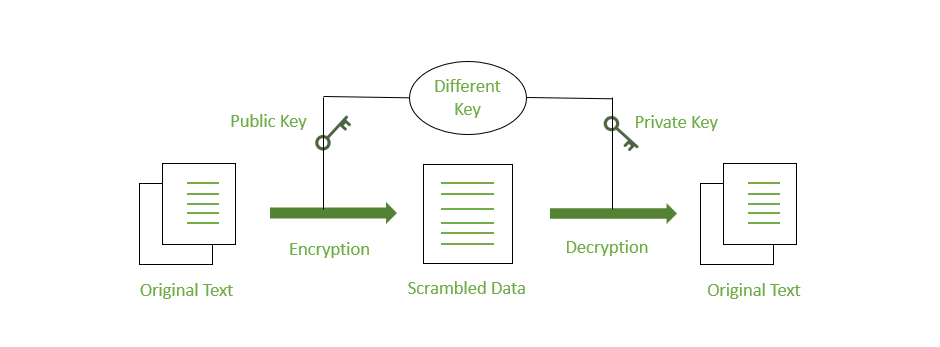
**Symmetric Key Encryption:**



*Symmetric 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.

**Asymmetric Key Encryption:**



*Asymmetric 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.

**States of Data Encryption:**

Data, whether it’s being transferred between users or stored on a server, is valuable and must be protected at all times.

**Data encryption in transit:**Information that is actively traveling 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. End-to-end encryption encrypts data throughout transmission, guaranteeing that it remains private even if intercepted.

**Encryption of data at rest:**Data at rest refers to information that is not actively moving from one device to another or from one network to another, such as information stored on a hard drive, laptop, flash drive, or archived/stored in another way. Due to device security features restricting access, data at rest is often less vulnerable than data in transit, but it is still vulnerable. It also contains more valuable information, making it a more appealing target for criminals.

Data encryption at rest reduces the risk of data theft 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?**

Assume a person possesses a box containing a few documents. The individual looks after the box and secures it with a lock. The individual sends this box of paperwork to his or her pal after a few days. The key is also kept by a buddy. This signifies that both the sender and the recipient have the same key. The buddy has now been given permission to open the box and see the document. The encryption method is the same as we mentioned in the sample. Encryption is performed on digital communications, though. 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.

The security of networks is intimately related to encryption. Encryption is useful for concealing data, information, and things that are incomprehensible to a normal human. Because both encryption and decryption are effective ways of cryptography, which is a scientific procedure for performing secure communication, the encrypted information may be transformed back to its original condition following the decryption process. There are a variety of algorithms for data encryption and decryption. However, “keys” can also be utilized to obtain high-level data security.

**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.

Given the importance of data security, many organizations, governments, and businesses require data to be encrypted in order to protect the company or user data. Employees will not have unauthorized access to user data as a result of this.

**Advantages of Data Encryption:**

1. Encryption is a low-cost solution.
2. 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.
3. Regulatory Fines Can Be Avoided With Encryption
4. Remote Workers Can Benefit from Encryption
5. Encryption improves the security of our information.
6. Consumer Trust Can Be Boosted by Encryption

**Disadvantages of Data Encryption:**

1. 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.
2. 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.
3. 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.

**Examples of 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)**](https://www.geeksforgeeks.org/data-encryption-standard-des-set-1/) 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.