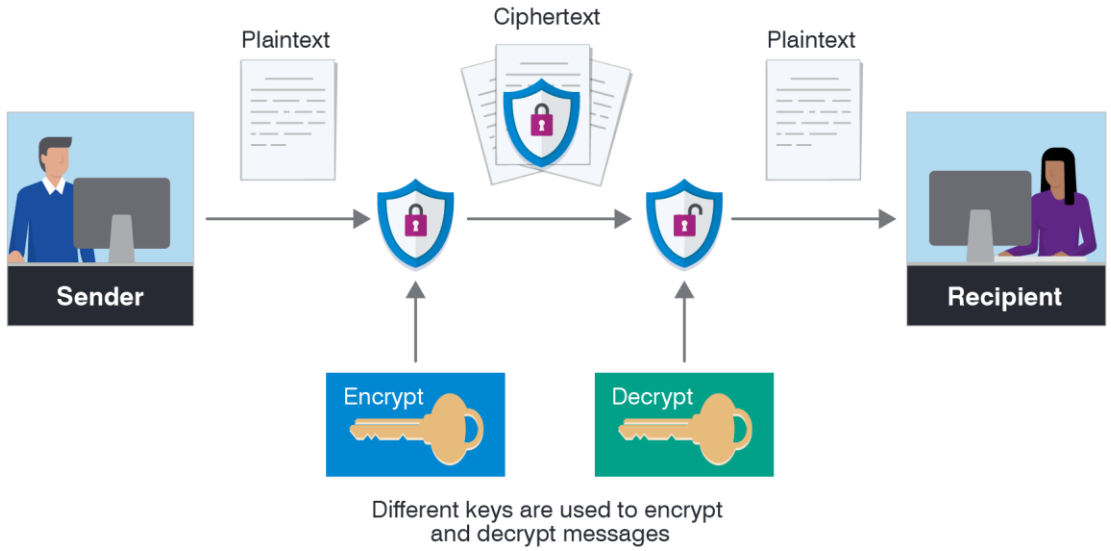
What is encryption?

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*.

Encryption has long been used to protect sensitive information. Historically, it was used by militaries and governments. In modern times, encryption is used to protect data both at rest and in motion. At-rest data is the type stored on computers and storage devices. In-motion data refers to data in transit between devices and over networks.



How Does Encryption Work?

Encryption converts human-readable plaintext into incomprehensible text, known as “ciphertext.” Encryption works by encoding plaintext into ciphertext using cryptographic mathematical models known as algorithms. Decoding the data back to plaintext requires using a decryption key, a string of numbers, or a password also created by an algorithm.

Why Is Encryption So Important?

Encryption is essential to cybersecurity and data protection, as it protects private information and sensitive data and enhances the security of communication between client apps and servers. Encryption is critical to every organization because it protects confidential data by converting it into ciphertext.

Encryption Types / Methods

There are two commonly used types of encryption: symmetric and asymmetric encryption.

Symmetric Encryption

Symmetric encryption is a simpler type that uses the same key for both encryption and decryption. This means that the sender and recipient must have access to the same key to decrypt the data. Symmetric encryption is faster and more efficient than asymmetric encryption, making it the preferred method for transmitting data in bulk. Common symmetric encryption methods include

Advanced Encryption Standard (AES), Data Encryption Standard (DES), and Triple Data Encryption Standard (3DES).

Asymmetric Encryption

Asymmetric encryption, also known as public-key cryptography, uses two separate keys for the encryption process. One key is the public key used to encrypt the data, while the other is the private key used to decrypt the data. The owner keeps the private key secret, while the public key is either shared among authorized recipients or made available to the public. Data that's encrypted using the recipient's public key can only be decrypted with the corresponding private key. Asymmetric encryption is slower and more complex than symmetric encryption, but it is more secure and eliminates the need for a secure key exchange. Common asymmetric encryption methods include RSA and Elliptic Curve Cryptography (ECC).

Hashing is another technique used in encryption, but it is not a form of encryption. Hashing generates a fixed-length value summarizing a file or message's contents. It is used to verify data integrity and detect unauthorized changes to data.

Symmetric Cipher Model:

A symmetric encryption scheme has five ingredients

• Plaintext: This is the original intelligible message or data that is fed into the algorithm as input.

• Encryption algorithm: The encryption algorithm performs various substitutions and transformations on the plaintext.

• Secret key: The secret key is also input to the encryption algorithm. The key is a value independent of the plaintext and of the algorithm. The algorithm will produce a different output depending on the specific key being used at the time. The exact substitutions and transformations performed by the algorithm depend on the key.

• Ciphertext: This is the scrambled message produced as output. It depends on the plaintext and the secret key. For a given message, two different keys will produce two different ciphertexts. The ciphertext is an apparently random stream of data and, as it stands, is unintelligible.

• Decryption algorithm: This is essentially the encryption algorithm run in reverse. It takes the ciphertext and the secret key and produces the original plaintext.