Cryptography is the practice of securing communications from unauthorised individuals. Encryption algorithms transform the original message or plaintext into ciphertext that cannot be understood by outsiders. The use of a key enables authorised individuals to decrypt the message and access its contents, ensuring confidentiality. Cryptography also focuses on the randomness of encryption to make it difficult for anyone to guess the input or key of the algorithm. This helps to achieve secure and robust connections and enhance privacy. Advancements in cryptography make it challenging to break encryptions, allowing encrypted files, folders, and network connections to be accessible only to authorised users.

Cryptography revolves around four main objectives:

Confidentiality: Confidentiality guarantees that only the intended recipient can decipher the message and read its contents.

Non-repudiation: Non-repudiation ensures that the sender of the message cannot later deny their reasons for sending or creating the message.

Integrity: Integrity focuses on ensuring that the information within the message cannot be tampered with while in transit or storage.

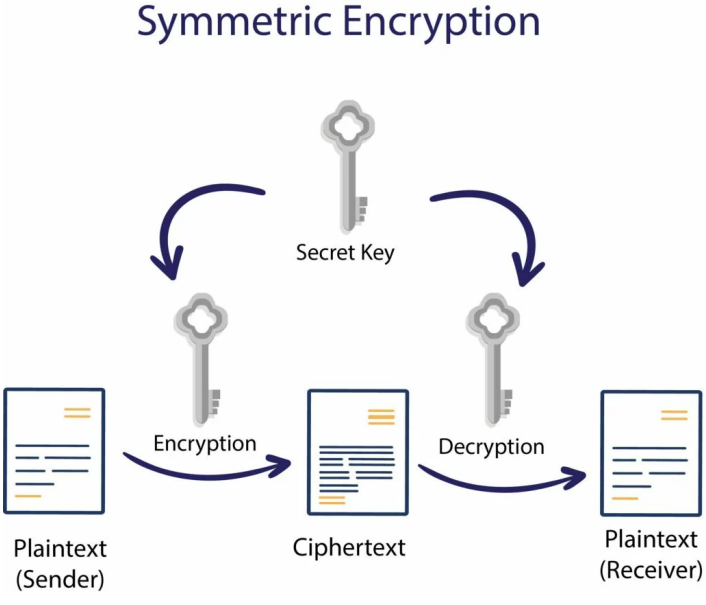
Authenticity: Authenticity verifies the identity of the sender and recipient and the message's destination, ensuring a secure and genuine transfer of information.

Cryptography has evolved from its beginnings with ciphers, starting with the Caesar Cipher. While ciphers were easy to decipher compared to modern cryptographic algorithms, they used keys and plaintext. Today's algorithms and cryptosystems are much more advanced and use multiple rounds of ciphers and encrypted ciphertext to ensure secure storage and transit of data. Some of the methods used today in cryptography are irreversible, ensuring the security of messages forever.

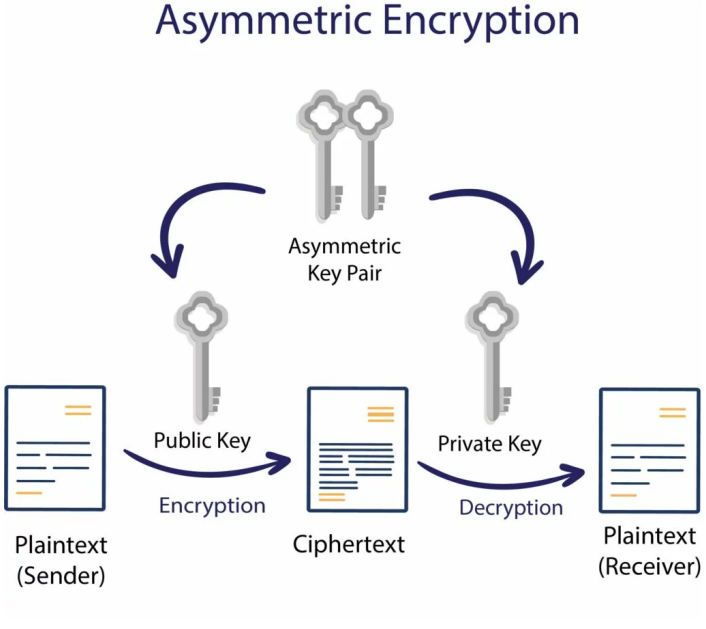
The need for more advanced cryptography methods arises from the increasing demand to protect data securely. Most of the ciphers and algorithms used in the past have been deciphered, rendering them useless for data protection. Today's algorithms can still be deciphered, but it could take years or even decades to decipher the meaning of just one message. Therefore, the race to develop newer and more advanced cryptography techniques continues.

Cryptography can be categorised into three types:

Secret Key Cryptography: This form of cryptography, also known as symmetric cryptography, uses a single key to encrypt and decrypt data. While this method is easy to use, it is generally only used for data at rest due to the risk of compromising the secret key during transit. Examples include AES, DES, and the Caesar Cipher.



Public Key Cryptography: This method, also known as asymmetric cryptography, uses two keys to encrypt and decrypt data. One key is used for encryption, while the other key decrypts the message. One key is kept private while the other is shared publicly. Examples include ECC, Diffie-Hellman, and DSS.



Hash Functions: Hash functions are one-way functions that protect data at the cost of not being able to recover the original message. A good hashing algorithm produces unique outputs for each input given, and the only way to crack a hash is by trying every input possible. Examples include MD5, SHA-1, SHA-2, SHA-3, Whirlpool, Blake 2, and Blake 3. Hashing is commonly used for data such as passwords and certificates.