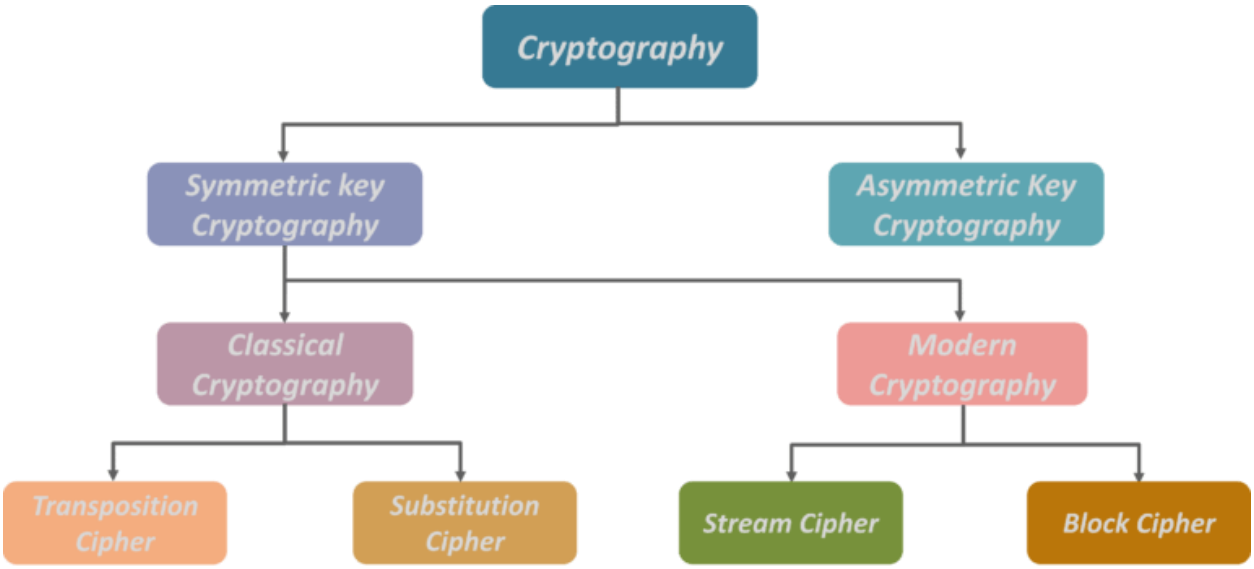
What is Cryptography?

Cryptography involves creating written or generated codes that allow information to be kept secret. Cryptography converts data into a format that is unreadable for an unauthorized user, allowing it to be transmitted without unauthorized entities decoding it back into a readable format, thus compromising the data.

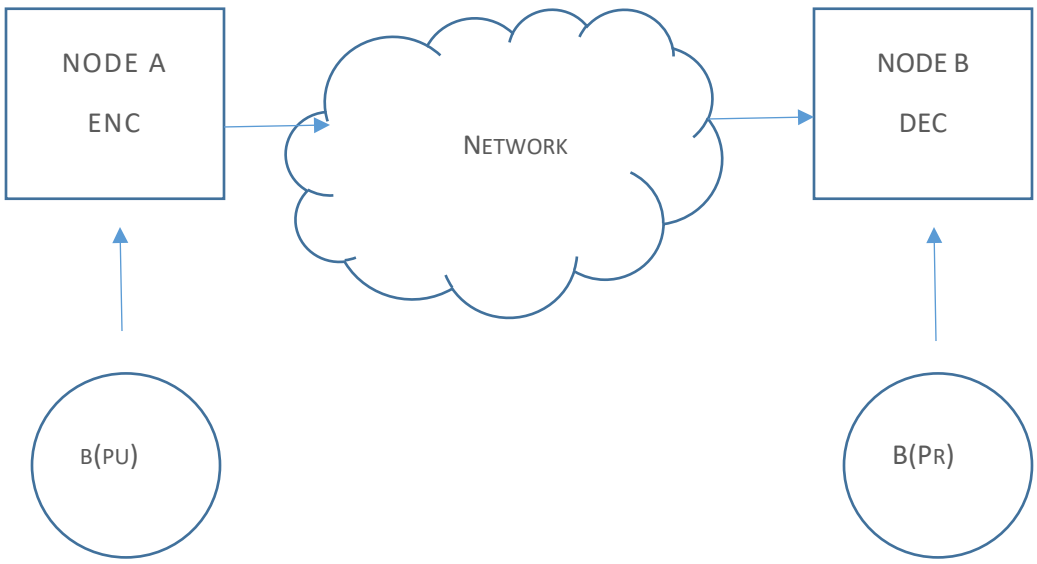
Cryptography is an important aspect when we deal with network security. 'Crypto' means secret or hidden. Cryptography is the science of secret writing with the intention of keeping the data secret. Cryptanalysis, on the other hand, is the science or sometimes the art of breaking cryptosystems. These both terms are a subset of what is called as Cryptology.

There are many aspects to security and many applications, ranging from secure commerce and payments to private communications and protecting health care information. One essential aspect for secure communications is that of cryptography. But it is important to note that while cryptography is *necessary* for secure communications, it is not by itself *sufficient*. The reader is advised, then, that the topics covered here only describe the first of many steps necessary for better security in any number of situations.

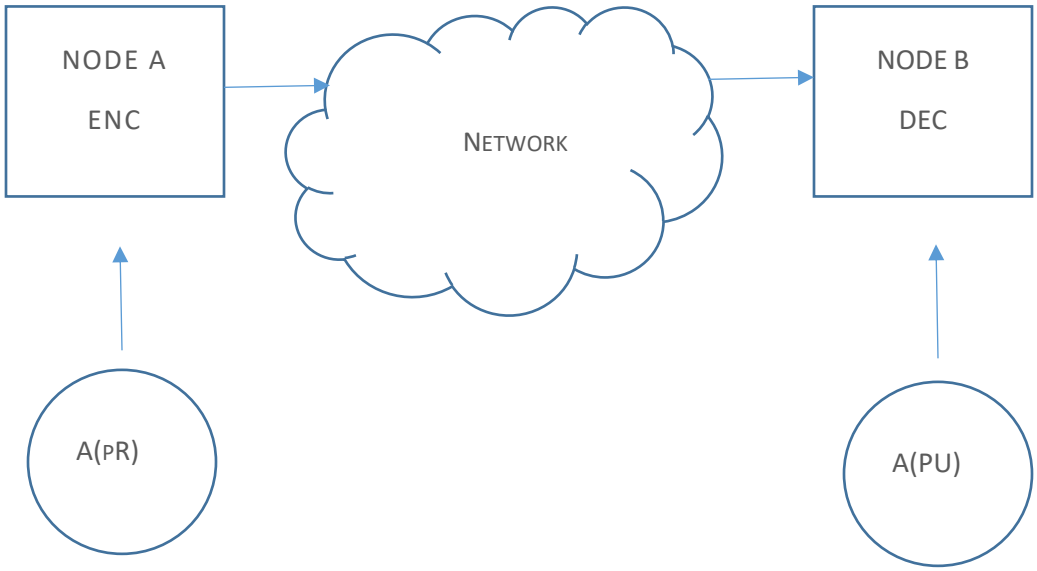


There are five primary functions of cryptography today:

1. *Privacy/confidentiality:* Ensuring that no one can read the message except the intended receiver.



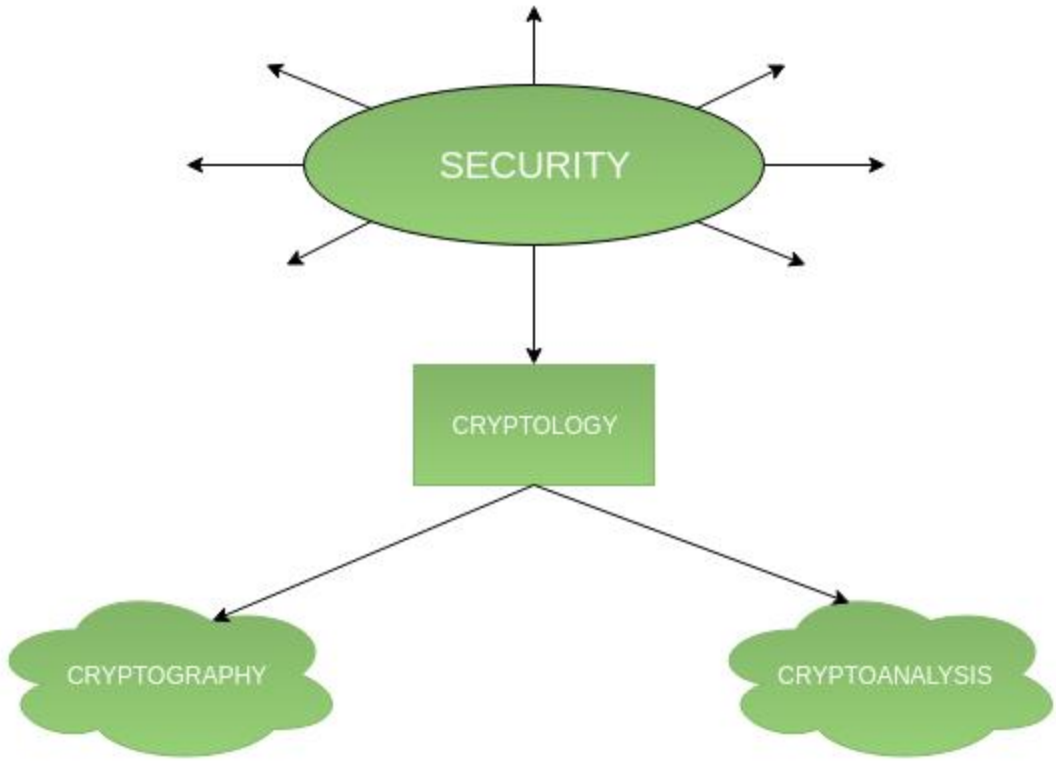
2. *Authentication:* The process of proving one's identity.



3. *Integrity:* Assuring the receiver that the received message has not been altered in any way from the original.
4. *Non-repudiation:* A mechanism to prove that the sender really sent this message.
5. *Key exchange:* The method by which crypto keys are shared between sender and receiver.

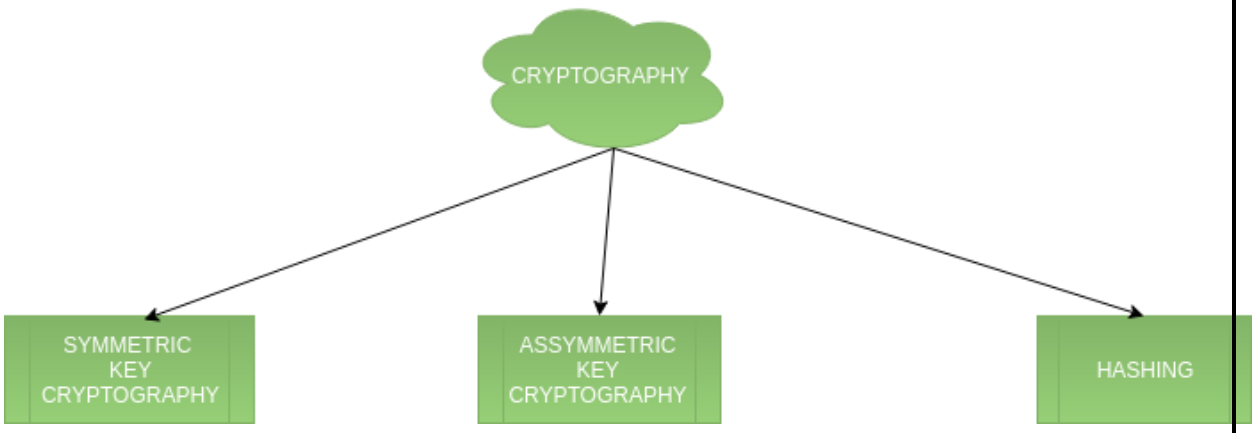
Classification –

The flowchart depicts that cryptology is only one of the factors involved in securing networks. Cryptology refers to study of codes, which involves both writing (cryptography) and solving (cryptanalysis) them. Below is a classification of the crypto-terminologies and their various types.

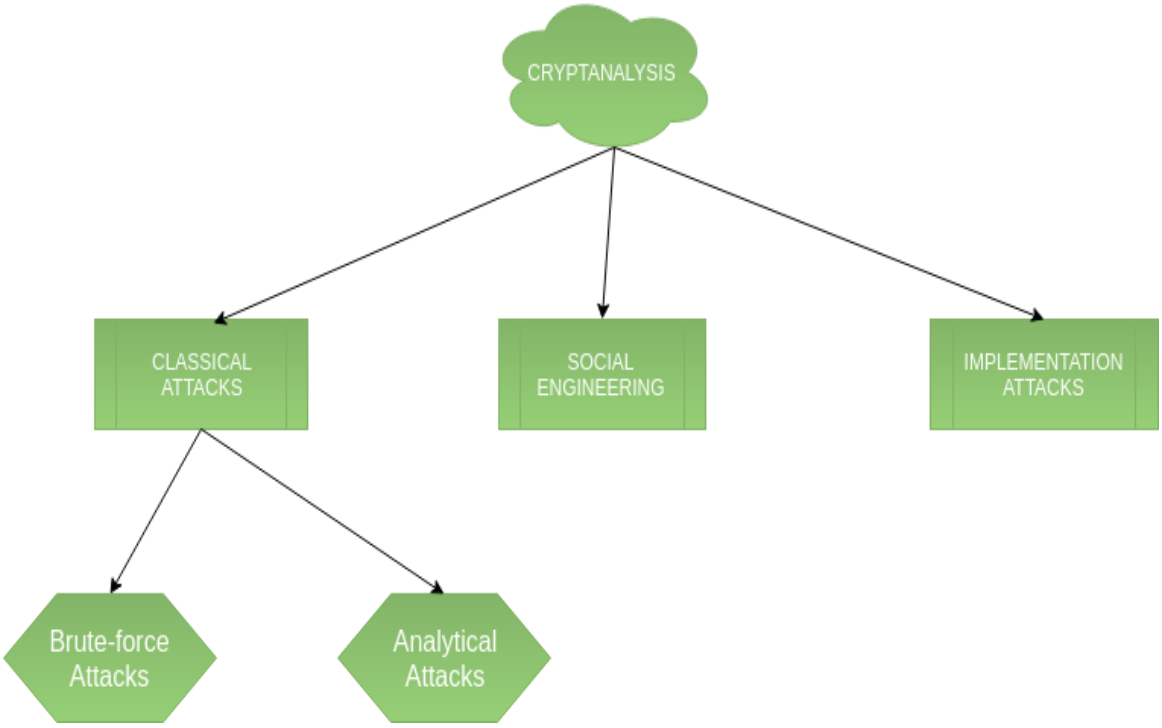


1. Cryptography –

   Cryptography is classified into symmetric cryptography, asymmetric cryptography and hashing. Below are the description of these types.



2. Cryptanalysis

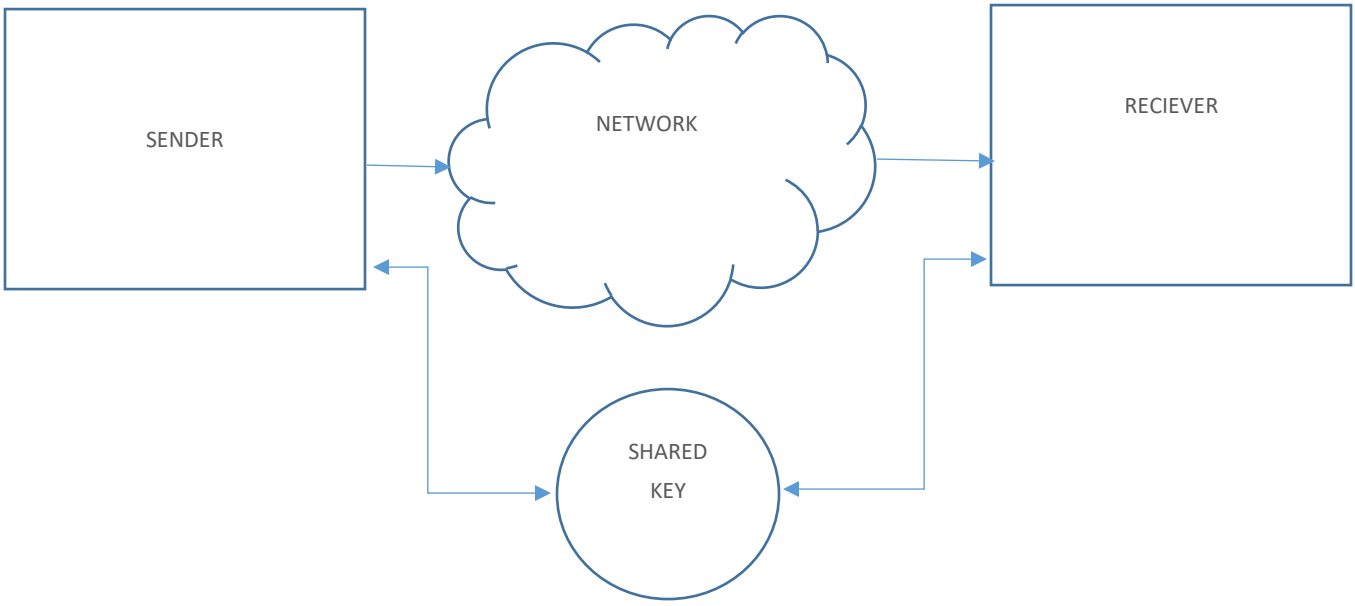


Symmetric Key Cryptography

In symmetric-key cryptography, we encode our plain text by mangling it with a secret key. Decryption requires knowledge of the same key, and reverses the mangling.

$$ciphertext = encrypt(plaintext, key)$$
$$plaintext = decrypt(ciphertext, key)$$

Symmetric key cryptography is useful if you want to encrypt files on your computer, and you intend to decrypt them yourself. It is less useful if you intend to send them to someone else to be decrypted, because in that case you have a "key distribution problem": securely communicating the encryption key to your correspondent may not be much easier than securely communicating the original text.



What is Symmetric Encryption Used For?

While symmetric encryption is an older method of encryption, it is faster and more efficient than asymmetric encryption, which takes a toll on networks due to performance issues with data size and heavy CPU use. Due to the better performance and faster speed of symmetric encryption (compared to asymmetric), symmetric cryptography is typically used for bulk encryption / encrypting large amounts of data, e.g. for database encryption. In the case of a database, the secret key might only be available to the database itself to encrypt or decrypt.

Some examples of where symmetric cryptography is used are:

- Payment applications, such as card transactions where PII needs to be protected to prevent identity theft or fraudulent charges
- Validations to confirm that the sender of a message is who he claims to be
- Random number generation or hashing

There are two types of symmetric encryption algorithms:

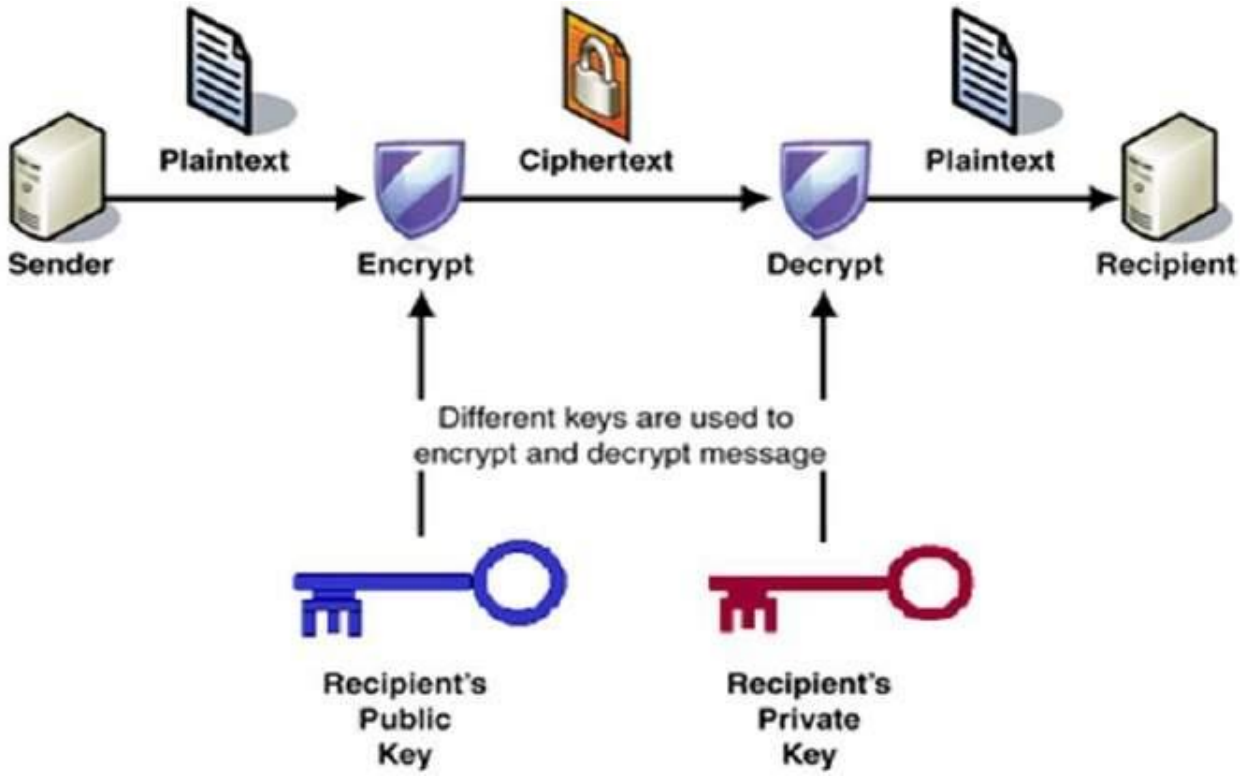
1. Block algorithms. Set lengths of bits are encrypted in blocks of electronic data with the use of a specific secret key. As the data is being encrypted, the system holds the data in its memory as it waits for complete blocks.
2. Stream algorithms. Data is encrypted as it streams instead of being retained in the system's memory.

Some examples of symmetric encryption algorithms include:

- AES (Advanced Encryption Standard)
- DES (Data Encryption Standard)
- IDEA (International Data Encryption Algorithm)
- Blowfish (Drop-in replacement for DES or IDEA)
- RC4 (Rivest Cipher 4)

Asymmetric Key Cryptography

Asymmetric cryptography, also known as public key cryptography, uses public and private keys to encrypt and decrypt data. The keys are simply large numbers that have been paired together but are not identical (asymmetric). One key in the pair can be shared with everyone; it is called the public key. The other key in the pair is kept secret; it is called the private key. Either of the keys can be used to encrypt a message; the opposite key from the one used to encrypt the message is used for decryption.



The most important properties of public key encryption scheme are −

- Different keys are used for encryption and decryption. This is a property which set this scheme different than symmetric encryption scheme.
- Each receiver possesses a unique decryption key, generally referred to as his private key.
- Receiver needs to publish an encryption key, referred to as his public key.
- Some assurance of the authenticity of a public key is needed in this scheme to avoid spoofing by adversary as the receiver. Generally, this type of cryptosystem involves trusted third party which certifies that a particular public key belongs to a specific person or entity only.
- Encryption algorithm is complex enough to prohibit attacker from deducing the plaintext from the ciphertext and the encryption (public) key.
- Though private and public keys are related mathematically, it is not be feasible to calculate the private key from the public key. In fact, intelligent part of any public-key cryptosystem is in designing a relationship between two keys.

Difference Between Symmetric and Asymmetric Encryption

- Symmetric encryption uses a singular key that must be shared among the people who need to receive the message while asymmetrical encryption uses a pair of public key and a private key to encrypt and decrypt messages when communicating.
- Symmetric encryption is an old practice while asymmetric encryption is relatively new.
- Asymmetric encryption was brought in to fix the inherent problem of the need to share the key in symmetrical encryption model, removing the need to share the key by using a pair of public-private keys.
- Asymmetric encryption eats up more time than the symmetric encryption.

When it comes to encryption, the latest systems may inevitably be the best fit. You should always use the encryption procedure that is applicable for the task at hand. In fact, as cryptography takes a new swing, new procedures are being established in a bid to catch up with the eavesdroppers and protect information to improve privacy. Hackers are destined to make it hard for experts in the coming years, thus expect more from the cryptographic community.