Cryptography and Cryptographic Algorithms

What is Cryptography?

Cryptography is a technique to secure data by writing or generating codes that make the information unreadable for the unauthorized individual.

It is derived from mathematical concepts and a set of rule-based calculations.

Cryptographic Algorithms usually involves three things:

- Cryptographic Key Generation
- Digital Signing
- Verification to Protect Privacy

Modern Cryptography includes Confidentiality, Integrity, Non Repudiation and Authentication.

Types of Cryptography

There are various types of Cryptography:

Symmetric Key Cryptography: It is an encryption scheme where a single common key is used by the sender and recipient of messages to encrypt and decrypt messages. Symmetric Key Schemes are quicker and easier, but the issue is that in a secure manner, sender and recipient have to swap key somehow. The Data Encryption System (DES) is the most common symmetric key cryptography system.

Asymmetric Key Cryptography: Under this scheme, information is encrypted and decrypted using a pair of keys. For encryption, a public key is used and a private key is used for decryption. The private key and the public key are unique. Even if the public key is known by everyone the intended receiver can only decode it because he/she alone knows the private key.

Symmetric Key Cryptography

Symmetric key cryptography creates a fixed length of bits which is known as a block cipher.

Block cipher usually encrypts one block of the bit rather than a single bit.

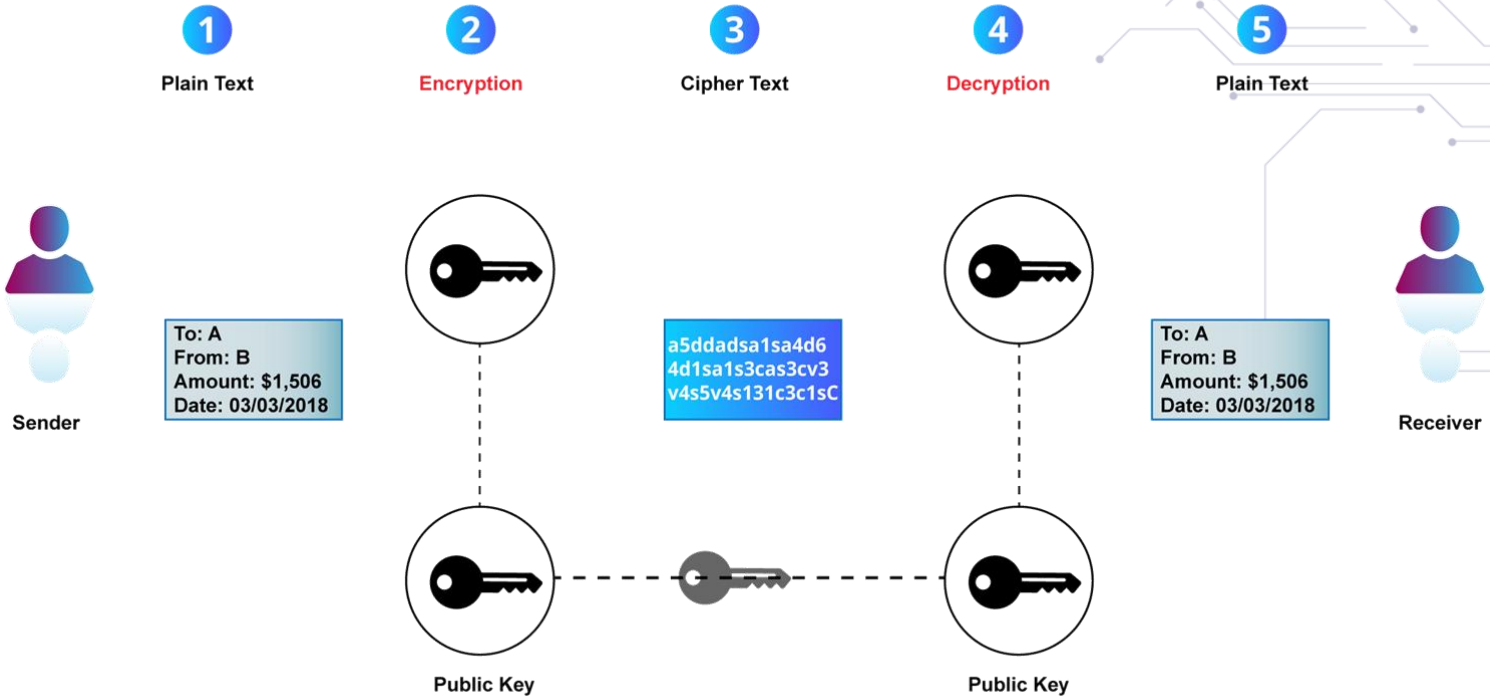
Block encrypted with one key cannot be decrypted with another symmetric key.

Symmetric-Key Cryptography is useful:

- When the algorithms are inexpensive to process.
- When the keys tends to be much smaller for the level of protection.
- When the user doesn't need to experience any time delay in the process of encryption and decryption.

Different kinds of Symmetric Key Cryptography algorithms are AES, DES, 3DES, Salsa, Seed, Aria.

Symmetric Cryptography



Asymmetric-Key Cryptography

Asymmetric-Key Cryptography usually works with two pair of keys, i.e. Public Key and Private Key.

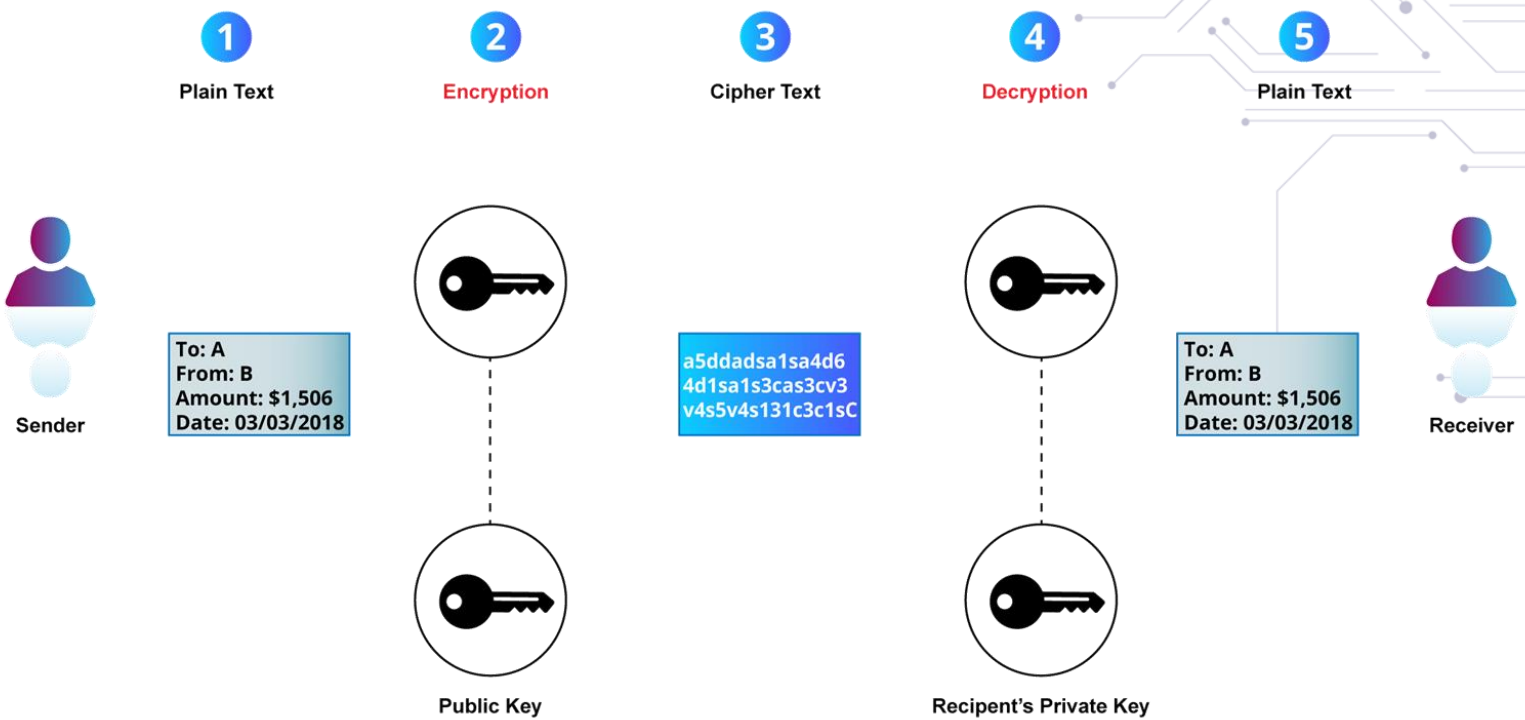
Public key can be shared or published to other individuals, private key must remain secret from others, as that same private key can only decrypt data encrypted by that same private key.

At present in Asymmetric-Key Cryptography there are typically two sized

- 1024 bits
- 2048 bits

Few types of asymmetric-key cryptography are Diffie Hellman, Digital Signature Algorithm, Elgamal, Elliptic Curve Cryptography, and many more.

Asymmetric Cryptography



Algorithms used in Blockchain Technology

Blockchain is a distributed database existing on various computers with a decentralized ledger tracking digital assets on the P2P network.

Two types of cryptographic algorithms are used for Blockchains - Asymmetric-key algorithms and Hash functions. Hash functions are used to provide any participant with the functionality of a single view of the blockchain. Generally, blockchains use the hashing algorithm SHA-256 as their hash function.

Blockchain is guarded by various Cryptographic Algorithms, namely:

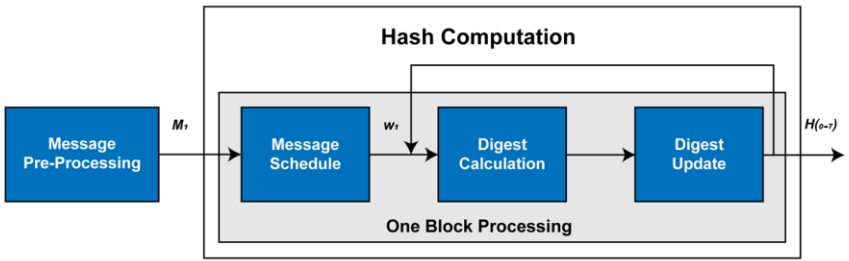
- SHA256
- Elliptic Curve Cryptography (ECC)
- RIPEMD160

SHA-256

Secure Hash Algorithms (SHA) are a family of cryptographic functions designed to keep data secure. It operates by using a hash function to transform the data: an algorithm consisting of bitwise operations, modular additions, and compression functions.

A fixed-size string that looks nothing like the original is then generated by the hash function. These algorithms are designed to be one-way functions, ensuring that it is nearly difficult to convert them back into the original data until they are converted into their respective hash values.

SHA-1, SHA-2, and SHA-3 are a few algorithms of this type, each of which was successively built in reaction to hacker assaults with progressively stronger encryption. Because of the commonly revealed bugs, SHA-0, for example, is now redundant.



Elliptic Curve Cryptography

In 1985, Neal Koblitz and Victor Miller independently suggested cryptography based on elliptic curves.

ECC is a strong cryptographic approach and is an alternative technique to RSA. It generates security through the mathematics of elliptic curves between key pairs for public key encryption.

ECC as well as RSA, is based on private-public key cryptography. However, with smaller key sizes, ECC provides the same security as RSA offers. It is less computer-intensive because ECC has smaller key sizes, so it is suitable for mobile devices and networks.

Symmetric Key Size (bits)	RSA and Diffie-Hellman Key Size (bits)	Elliptic Curve Key Size (bits)
80	1024	160
112	2048	224
128	3072	256
192	7680	384
256	15360	521

RIPEMD 160

RIPEMD 160 stands for RACE Integrity Primitives Evaluation Message Digest.

RIPEMD160 is a cryptographic function which is also based on Merkle-Damgard just like SHA-256.

Compression Function and Padding are the backbones of the RIPEMD160.

RIPEMD 160 is made up of 5 blocks that run 16 times which further adds up to 80 stages.

It is somewhat similar to SHA-256, but it is comparatively slower than the SHA-256.

There are four types of RIPEMD algorithms:

- RIPEMD-128
- RIPEMD-160
- RIPEMD-256
- RIPEMD-320

Blockchain Council™

THANK YOU!

Any questions?

Visit

community.blockchain-council.org

You can also mail us at

hello@blockchain-council.org