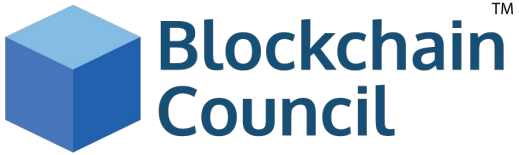


Certified Blockchain Architect

Cryptography and Blockchain Algorithms

What is Cryptography?

- A Cryptography is a technique to secure data by writing or generating codes which makes the information unreadable for the unauthorized individual
- Cryptography are usually used by people who are in computer security domain under various levels.
- Cryptographic techniques are 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
- Cryptography is very much similar to cryptology and cryptoanalysis
- Modern Cryptography includes Confidentiality, Integrity, Non Repudation and Authentication

Types of Cryptography

- There are various types of Cryptography namely
  - Symmetric Key Cryptography
  - Asymmetric Key Cryptography

Symmetric Key Cryptography

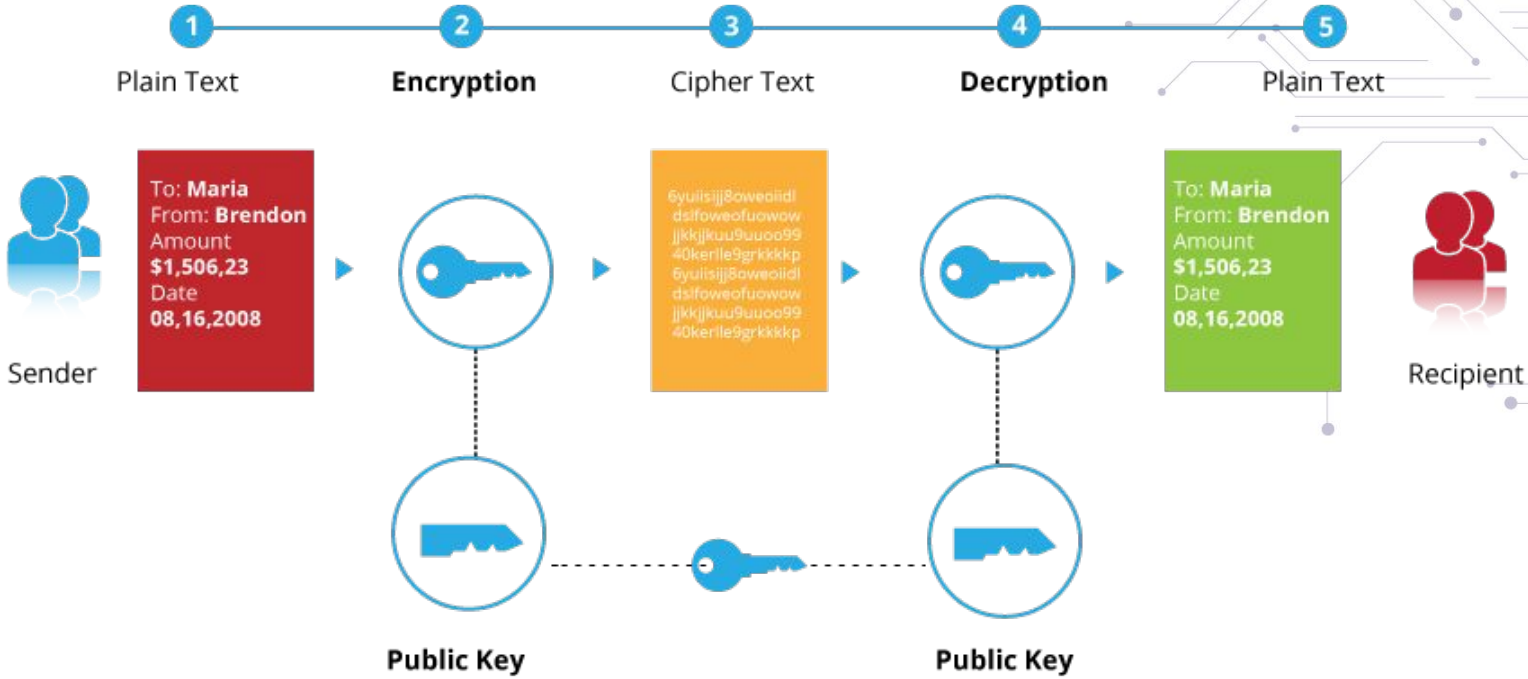
Symmetric-key Cryptography

- This type of cryptography create a fixed length of bits which is known as a block cipher.
- Blockcipher usually encrypts one block of bit rather than a single bit and is encrypted with secret key that the creator/sender uses to encipher data (encryption) and the receiver uses to decipher it.
- 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 you don’t want to experience any time delay in the process of encryption and decryption
- In the whole process the block encrypted with one key cannot be decrypted with another symmetric key.

Types of Symmetric-Key Cryptography

- Few Types of Symmetric-Key Cryptography are:
  - Data Encryption Standard
    - Triple DES (3DES)
    - DESX
  - Advanced Encryption Standard
  - CAST 128/256
  - International Data Encryption Algorithm(IDEA)
  - Rivest Ciphers (Ron's Code)
  - Blowfish
  - Salsa and ChaCha
  - Camelia
  - Kasumi
  - Seed
  - Aria

Symmetric Cryptography



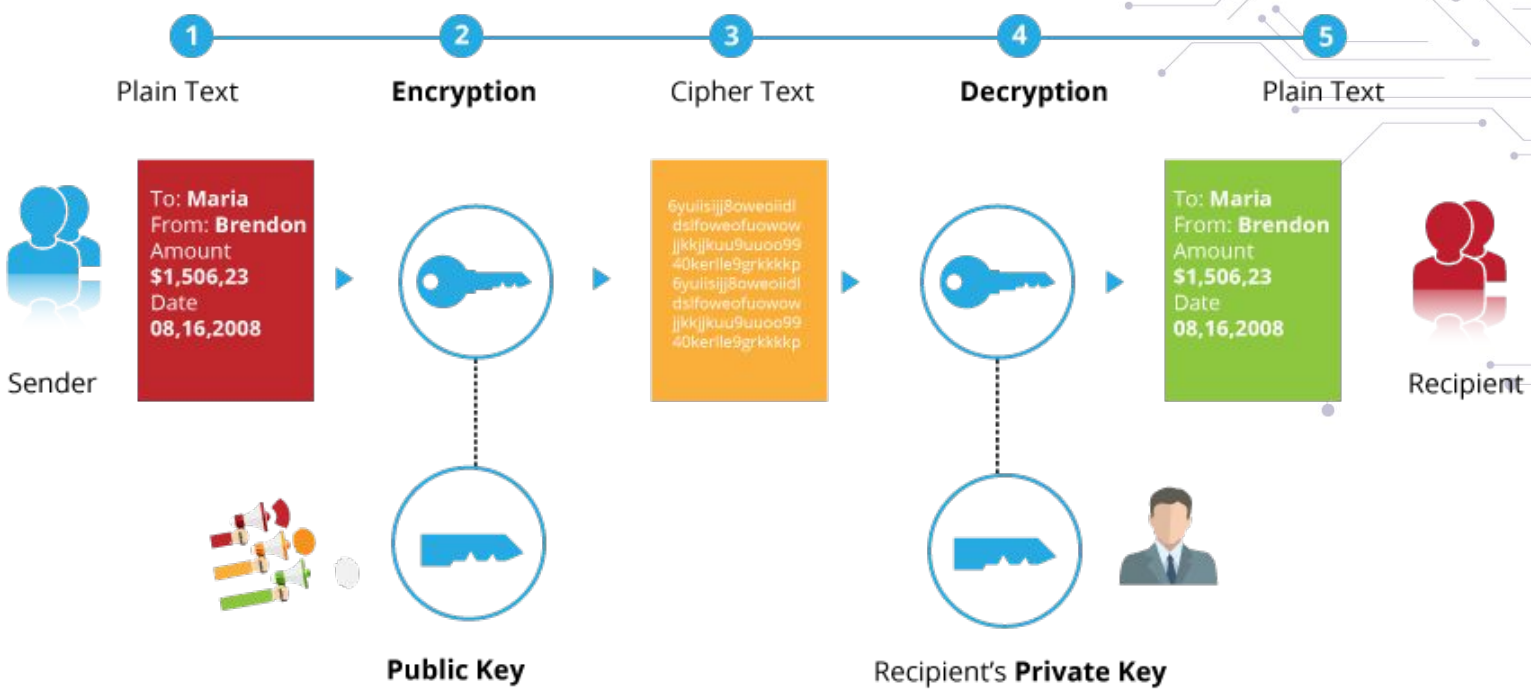
Asymmetric-Key Cryptography

- It is a most commonly used implementations presented by Rivest-Shamir-Adelman Data Security
- Asymmetric-Key Cryptography usually works with two pair of keys(i.e Public Key and Private Key), which are with an individual who needs to authenticate his identity electronically and to encrypt data.
- In Asymmetric-Key Cryptography, public key can be shared or published to other individuals but the private key must remain secret from others, because data encrypted by public key can only be decrypted by that same private key.
- At present in Asymmetric-Key Cryptography there are typically two sized
  - 1024 bits
  - 2048 bits
- Asymmetric-Key Cryptography is not always recommended for encrypting large amount of data, but instead can be used to encrypt data which is smaller than the length of the key.

Types of Asymmetric-Key Cryptography

- Few types of Asymmetric-Key Cryptography are:
  - Diffe-Helman
  - Digital Signature Algorithm (DSA)
  - Elgamal
  - Elliptic Curve Cryptography (ECC)
  - Carmer-Shoup
  - Key-Exchange Algorithm
  - LUC
  - McElice

Asymmetric Cryptography



Algorithms used in Blockchain Technology

- Blockchain is a distributed database existing on various computers with a decentralized ledger tracking digital assets on P2P network.
- Blockchain is guarded by various Cryptographic Algorithms namely:
  - SHA256
  - Elliptic Curve Cryptography (ECC)
  - RIPEMD160

SHA-256

- SHA-256 is a secure hash algorithms which was designed by NSA that contains 256-bit digest.
- It is a successor of SHA-1 and can also be referred to as SHA-2 which is one of the most secure hash algorithm.
- It is not more complex to code than SHA-1.
- SHA-256 provides secure communications through the file name known as ‘Certificates’.
- In SHA-256, the information is broken down into 512-bits, and produces ‘cryptographic mix’ and then attaches 256-bit hash code. This algorithm involves simple rounds which is repeated 64 times.
- SHA-256 is build on the Merkle-Damgard construction method, which converts the initial index into the blocks after the changes are made.

Elliptic Curve Cryptography

- ECC is defined as a curve that is completely non-singular and there is a line between two points on this curve which will always intersect at a third point.It is represented as an algebraic structure which offers the same security as RSA, but at smaller footprint.
- ECC contains many different curve and the curve used in blockchain are '**secp256k1**' which is the most widely used method for digital signature schemes.
- ECC was introduced back in 1985 by Neal Koblitz and Victor Miller.
- ECC uses a trapdoor function which allows going from A -> B easily but going back to B -> A is considered as infeasible
- ECC in nature relies on the concept of Point Multiplication, where the multiplicand will represent a private key so it becomes infeasible to compute from the given starting points.

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 backbone of the RIPEMD160
- RIPEMD 160 is made up of 5 blocks that runs 16 times which is further adds up to 80 stages.
- It is somewhat similar to SHA-256, but it is comparatively slower than the SHA-256

THANK YOU!

Any questions?

You can mail us at

hello@blockchain-council.org