Cryptography and Cryptographic Algorithms

What is Cryptography?

Cryptography is a technique to secure data using computer software.
It works such that users can encrypt and decrypt the transaction so that the data is not leaked to third party.
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

In the case of blockchain, cryptography is used to encrypt transaction data to maintain the confidentiality and authenticity of transaction data.

Types of Cryptography

There are various types of Cryptography:

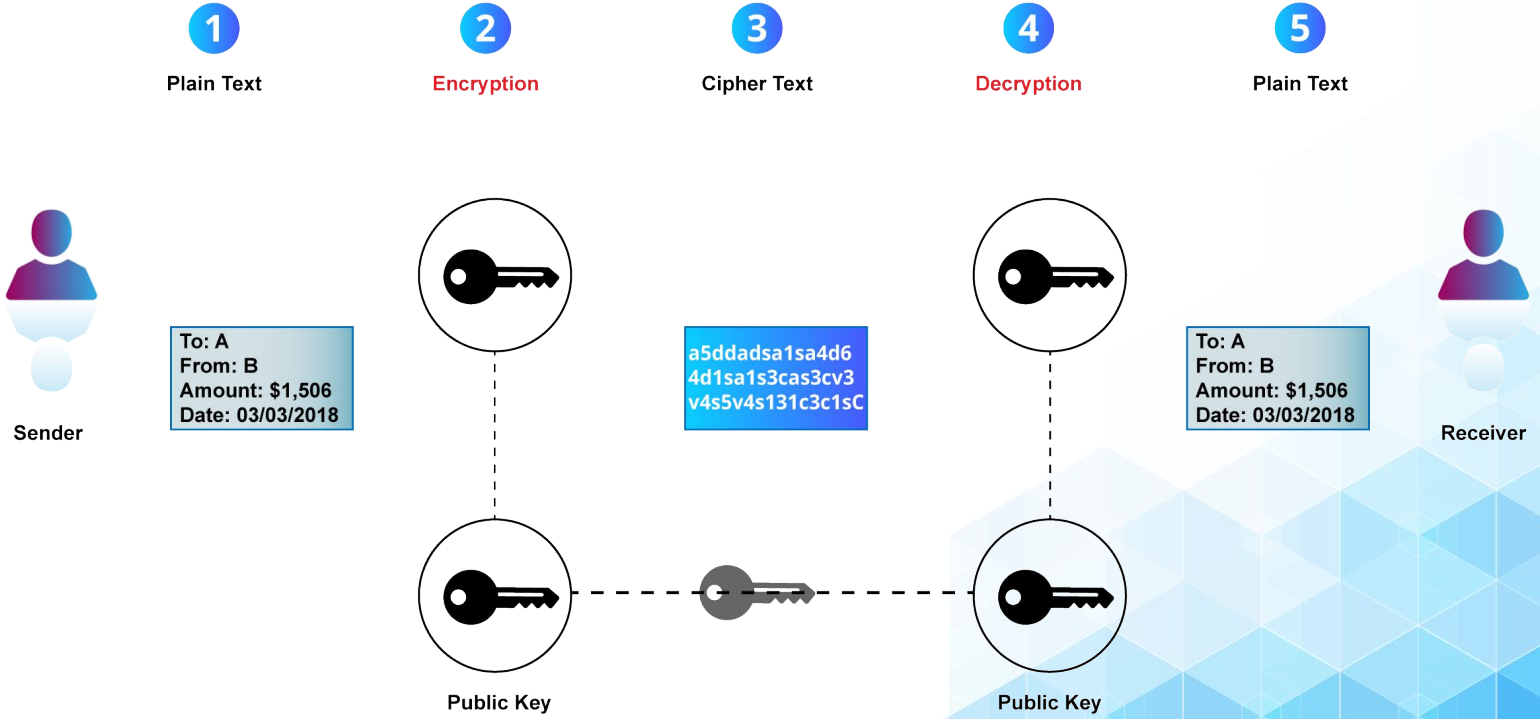
Symmetric Key Cryptography: It is an encryption scheme where a single common key is used by the sender and recipient of messages to encrypt and decrypt messages. Symmetric Key Schemes are quicker and easier to use. The speed is achieved on compromise of security as it is very difficult to exchange key between two people without revealing some hidden information.

Asymmetric Key Cryptography: In this method, encryption and decryption is done 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 they alone know the private key.

Symmetric Key Cryptography

- Symmetric key cryptography uses single key for encryption and decryption.
- Symmetric key encryption can be divided into two parts.
  - Block
  - stream
- Block cipher usually encrypts a fixed size chunk of data.
- On other hand Stream cipher encrypts data byte-by-byte.
- Different kinds of symmetric key cryptography algorithms are AES, DES, 3DES, Salsa, Seed, and Aria.

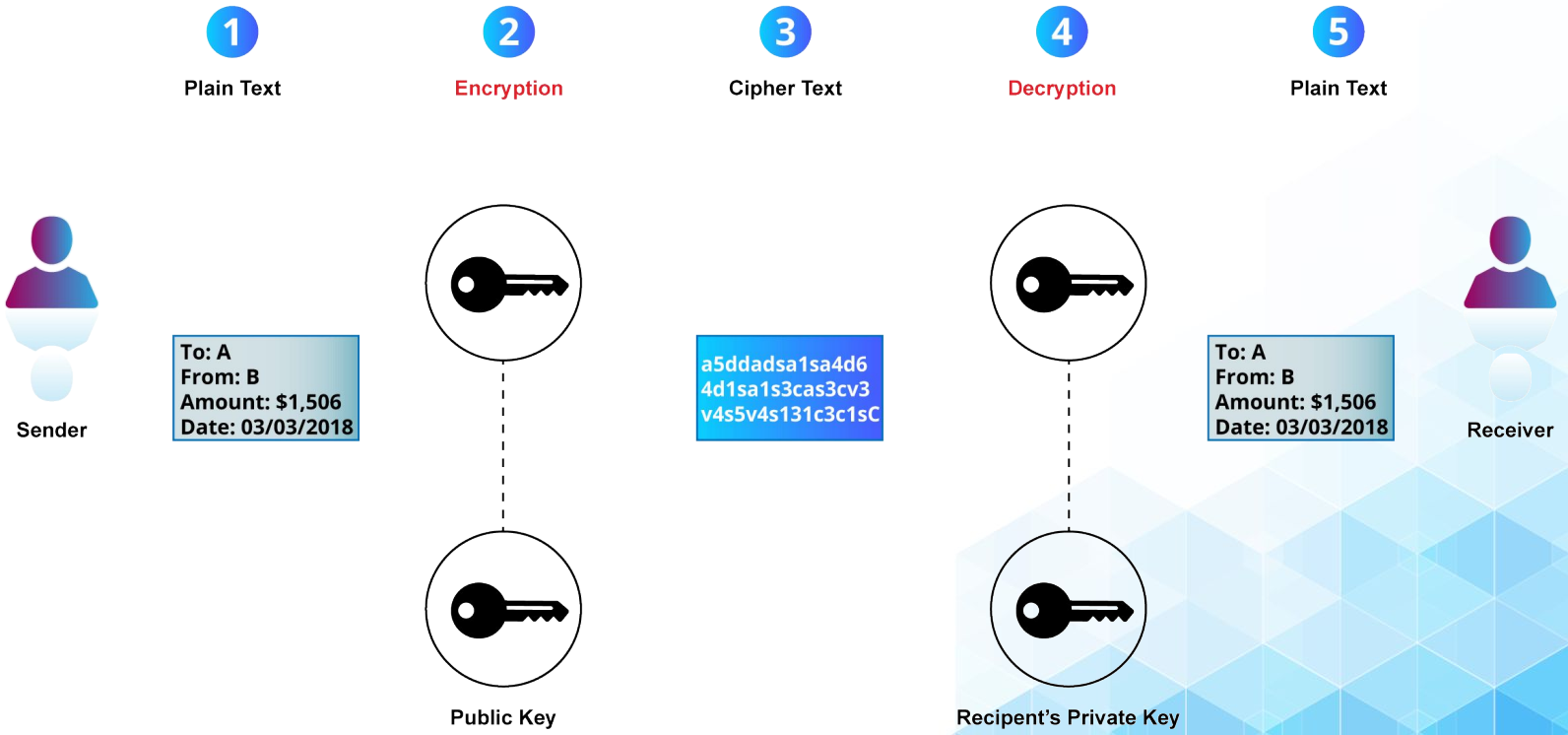
Symmetric Cryptography



Asymmetric-Key Cryptography

- Asymmetric-Key Cryptography usually works with two pair of keys, i.e. Public Key and Private Key.
- A public key can be shared or published to other individuals. A private key is kept secret.
  Public keys are used to only encrypt data and private keys can decrypt data.
- There are many Asymmetric key encryption used, some are:
  - Rivest Shamir Adleman (RSA)
  - Digital Signature Algorithm (DSA)
  - Elliptic Curve Cryptography (ECC)
  - Elgamal

Asymmetric Cryptography



Algorithms used in Blockchain Technology

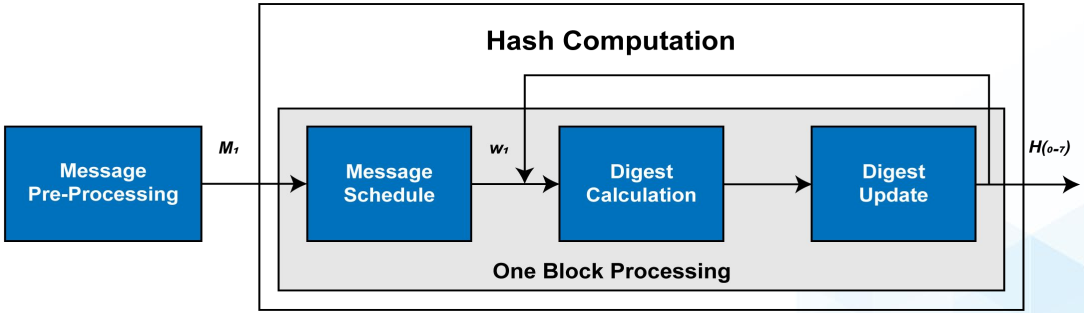
Blockchain is a distributed database existing on various computers with a decentralized ledger tracking digital assets on the P2P network.

Some of the most popular encryption standard in blockchain are:

- SHA256
- Elliptic Curve Cryptography (ECC)
- RIPEMD-160

SHA-256

- Secure Hash Algorithms (SHA) operates by using a hash function.
- SHA 256 produces a 256 bits fixed length output.
- Hash functions are one way functions that are used to create fixed length (output) from any variable length input.
- These algorithms are one-way functions, making it nearly impossible to get the input data from the output.



Elliptic Curve Cryptography (ECC)

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

ECC uses a private key on top of that curve, the mirror of that private key point on the curve will be your public key.

ECC is based on private-public key cryptography and with smaller key sizes, ECC is less computer-intensive.

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.
- It is a cryptographic function which is also based on Merkle-Damgard, just like SHA-256.
- It is made up of 5 blocks that run 16 times, which further adds up to 80 stages.
- 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

Mail Us

hello@blockchain-council.org