BLOCKCHAIN TUTORIAL 5

Symmetric keys and asymmetric keys

BLOCKCHAIN TUTORIAL 5

Symmetric keys and asymmetric keys

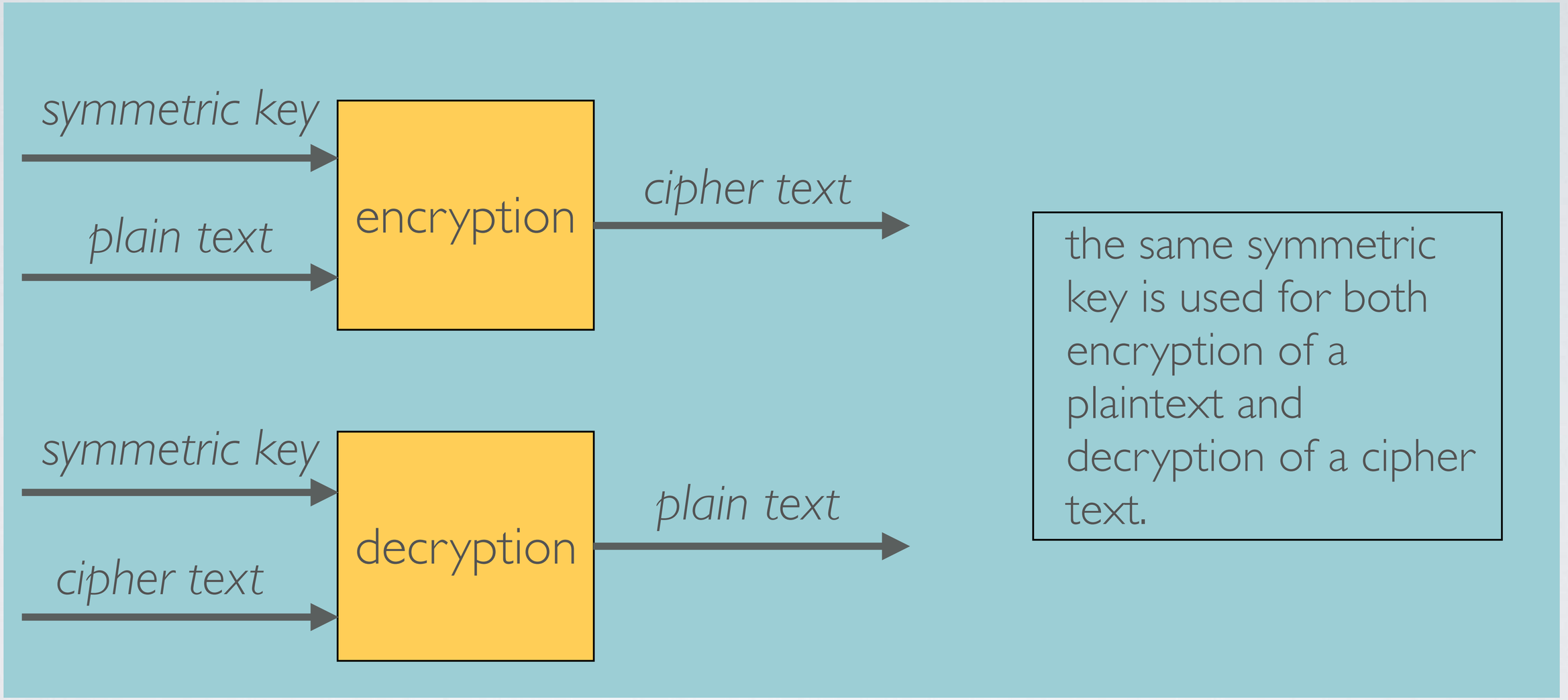
SYMMETRIC AND ASYMMETRIC

- There are two basic techniques to encrypt/decrypt information:
  - ✦symmetric encryption/decryption
  - ✦asymmetric encryption/decryption

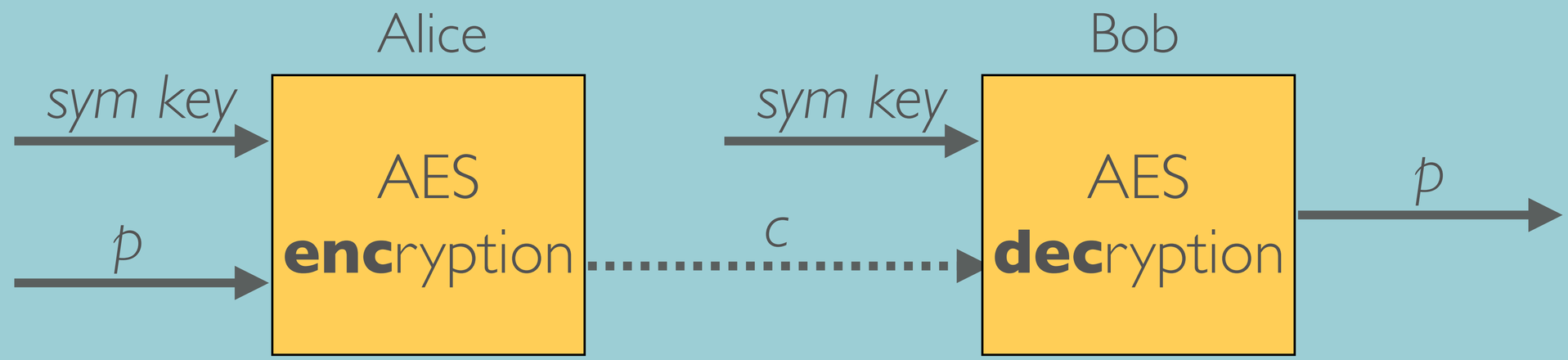
SYMMETRIC KEY

- A symmetric key algorithm requires the **same key** for both encryption of a plaintext and decryption of a cipher text.
- This same key is also called a shared secret.
- Symmetric key algorithms are generally much faster (hundreds to thousands times) to encrypt and decrypt a message than asymmetric key algorithms.
- Big disadvantage of using a symmetric key algorithm is that both sender (Alice) and receiver (Bob) needs to know the shared secret.
- Few symmetric key algorithms: AES (Advanced Encryption Standard), Triple DES (Data Encryption Standard)

SYMMETRIC KEY



SYMMETRIC KEY



Alice ENC(p, sym key) = c ⋯▶ Bob DEC(c, sym key) = p

ASYMMETRIC KEY

- An asymmetric key algorithm requires **two keys** called a public and a private key. One of the key is used for encryption of a plaintext and the other key is used for decryption of the cipher text.

- If Alice generates a private key and a corresponding public key, than anyone is allowed to know her public key, but Alice must keep her private key secret.

- A big disadvantage is that asymmetric key algorithms are generally much slower (hundreds to thousands times) to encrypt and decrypt a message than symmetric key algorithms.

- The advantage of using an asymmetric key algorithm is that any sender can encrypt a message using the receiver public key, but only the receiver can decrypt the cipher text using its private key.

ASYMMETRIC KEY

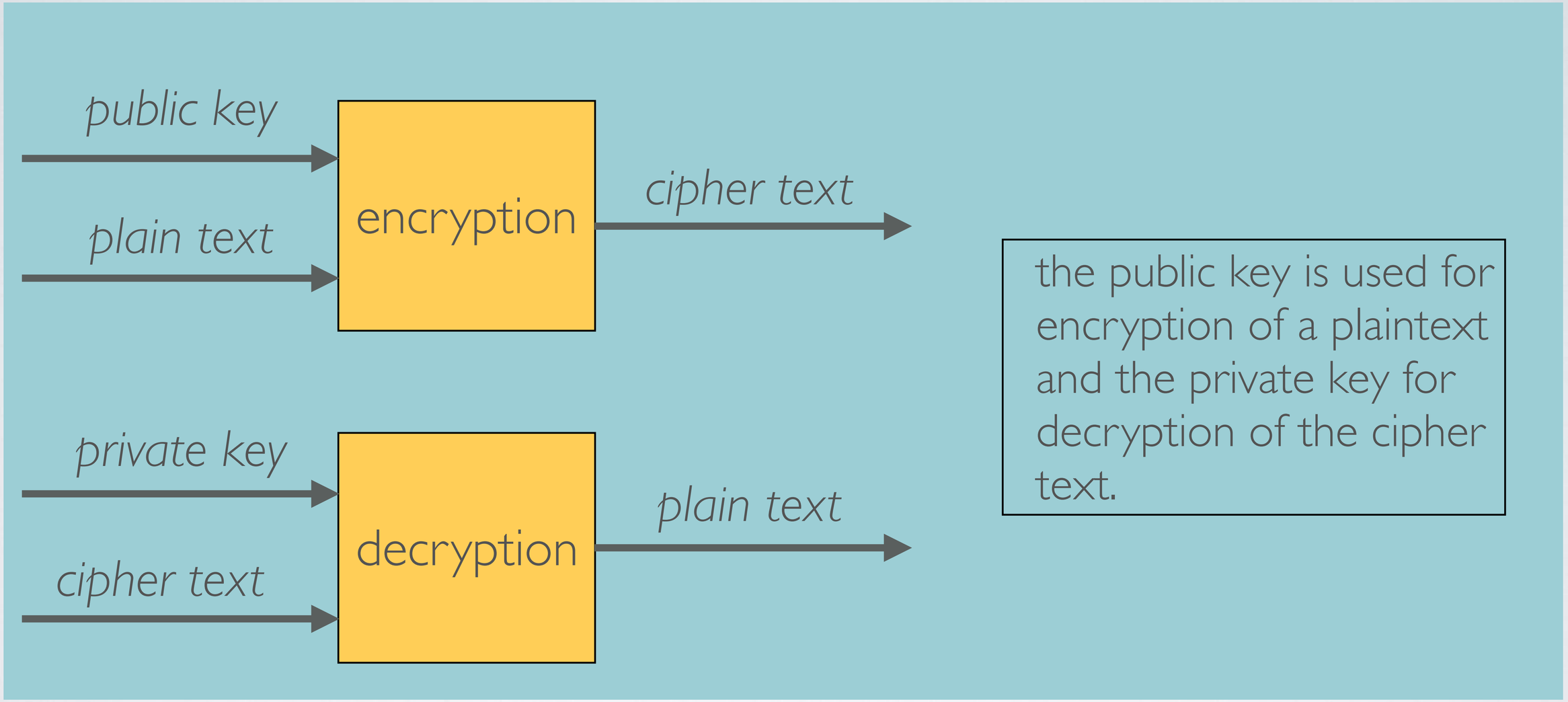
- A public key and private key are mathematically interconnected. Meaning each public key has only one corresponding private key.

- Few asymmetric key algorithms: RSA (Rivest Shamir Adleman), ECDSA

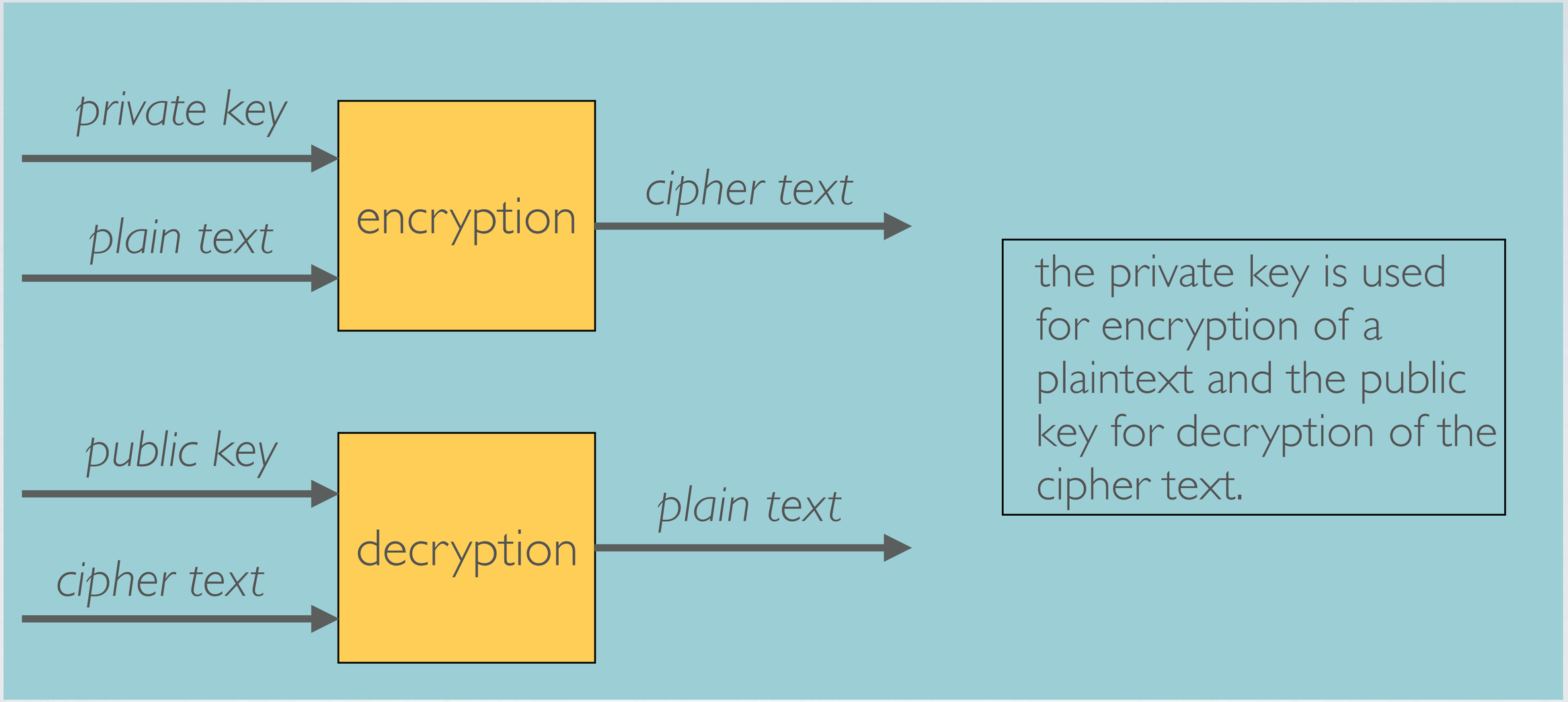
  (Elliptic Curve Digital Signature Algorithm)

- In Blockchain the Elliptic Curve Digital Signature Algorithm is often used.

ASYMMETRIC KEY



ASYMMETRIC KEY



the private key is used for encryption of a plaintext and the public key for decryption of the cipher text.

ASYMMETRIC KEY