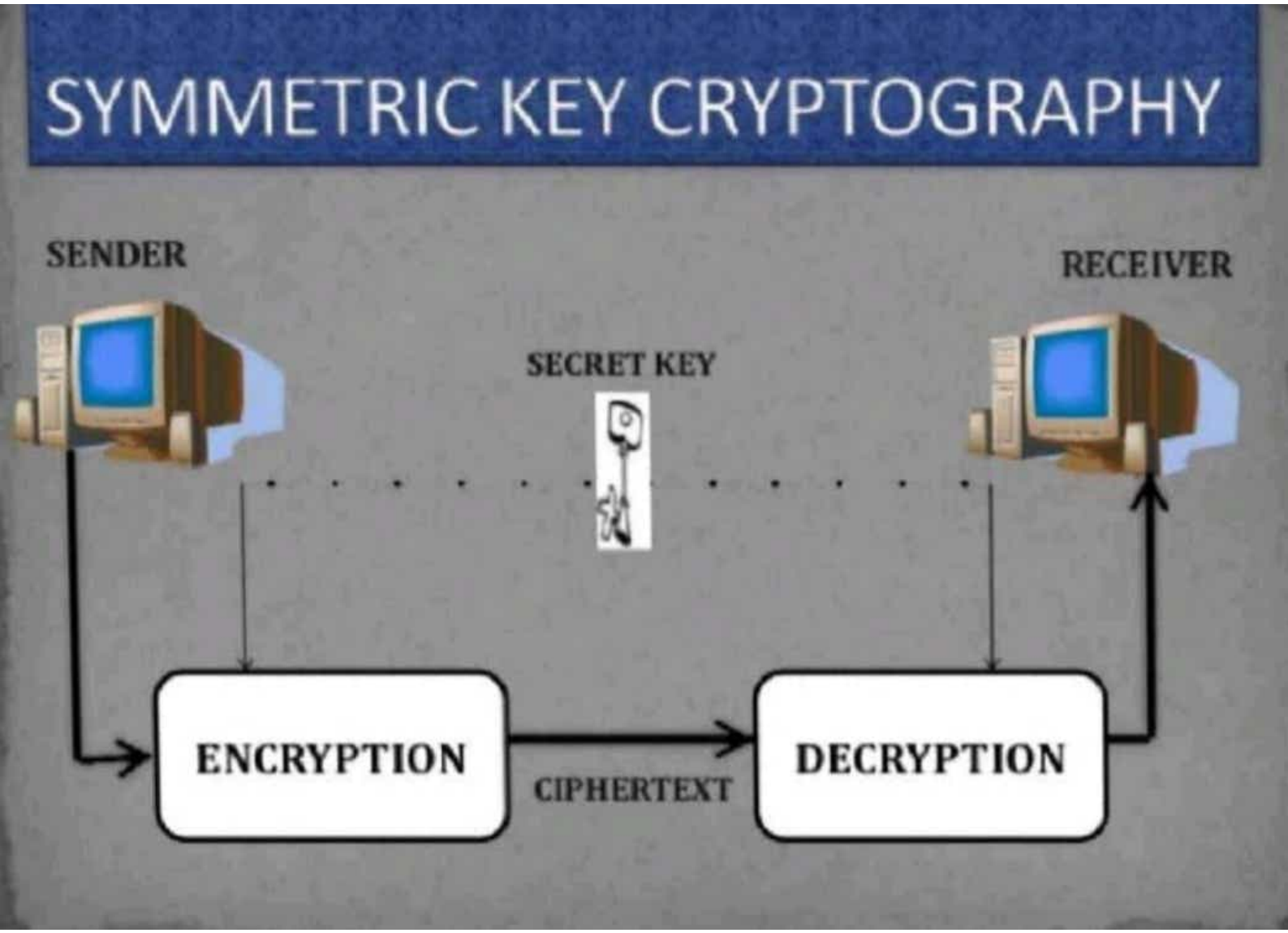
CRYPTOGRAPHY

- Cryptography is the science and art of transforming messages to make them secure and immune to attack.

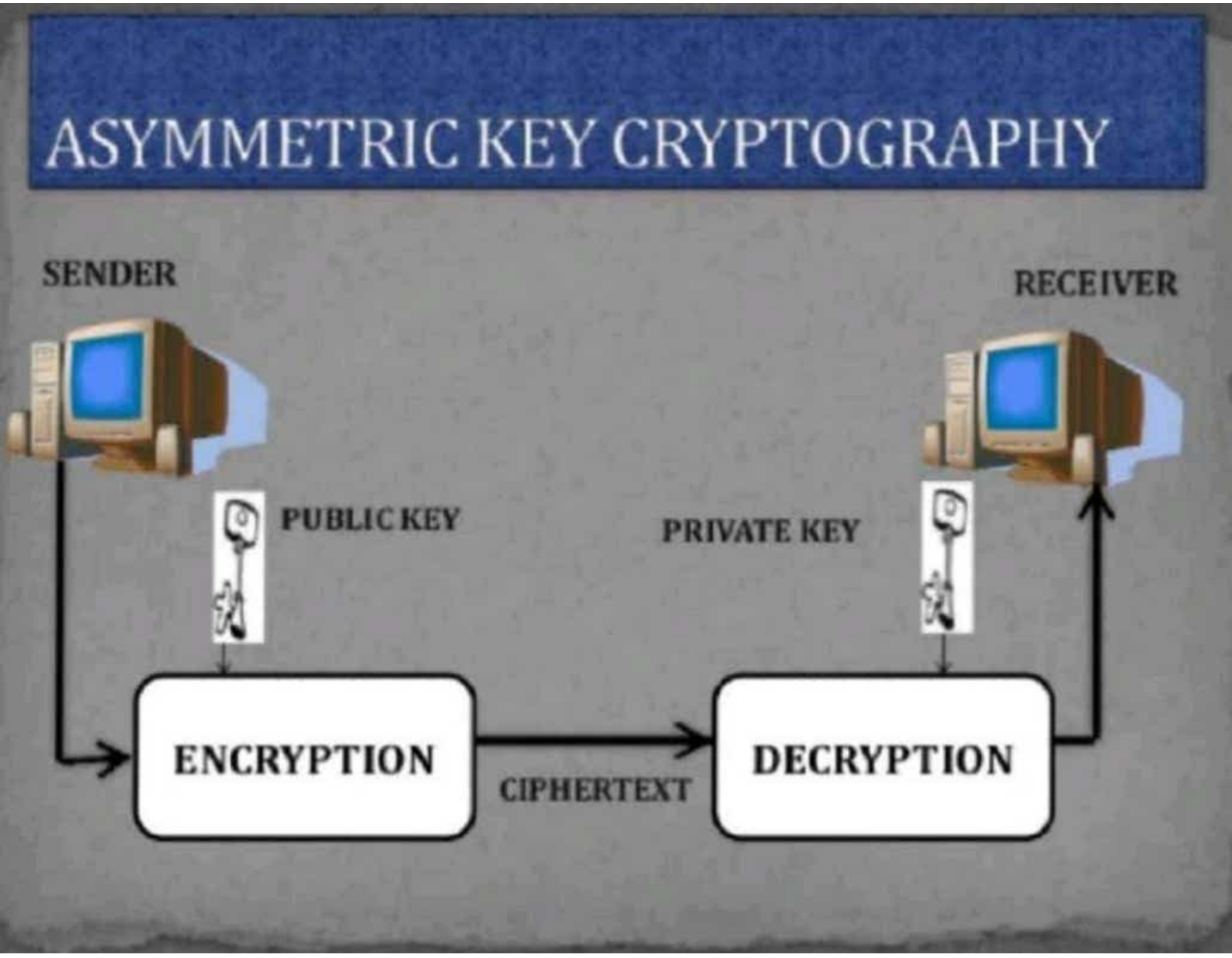
SYMMETRIC KEY CRYPTOGRAPHY

- Also known as secret key. Sender & receiver uses same key & an encryption/decryption algorithm to encrypt/decrypt data. i.e. the key is shared.


SYMMETRIC KEY CRYPTOGRAPHY
SENDER
RECEIVER
SECRET KEY
ENCRYPTION
CIPHERTEXT
DECRYPTION

ASYMMETRIC KEY CRYPTOGRAPHY

- Also known as public key cryptography. Sender & receiver uses different keys for encryption & decryption namely PUBLIC & PRIVATE respectively.


ASYMMETRIC KEY CRYPTOGRAPHY
SENDER
RECEIVER
PUBLIC KEY
PRIVATE KEY
ENCRYPTION
CIPHERTEXT
DECRYPTION

COMPARISON

SYMMETRIC KEY CRYPTOGRAPHY	ASYMMETRIC KEY CRYPTOGRAPHY
1) The same algorithm with the same key is used for encryption and decryption.	1) One algorithm is used for encryption and decryption with a pair of keys, one for encryption and one for decryption.
2) The key must be kept secret.	2) One of the two keys must be kept secret.
3) It may be impossible or at least impractical to decipher a message if no other information is available.	3) It may be impossible or at least impractical to decipher a message if no other information is available.

What is Digital Signature?

- **Digital Signature** is a type of asymmetric cryptography used to simulate the security properties of a signature in digital, rather than written, form.

- **Digital Signature** is an electronic signature that can be used to authenticate the identity of the sender of a message or the signer of a document, and possibly to ensure that the original content of the message or document that has been sent is unchanged.