Open

INFORMATION SECURITY

Fundamentals

CRYPTOGRAPHY

Cryptography is a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it.

Cryptography is closely related to the disciplines of cryptology and cryptanalysis. It includes technologies such as microdots, merging words with images, and other ways to hide information.

TERMINOLOGY

Plaintext

👉 A message that is going to be transmitted or stored in plain text. Anyone can read plaintext.

Encryption

👉 The method by which we can hide the actual meaning of plaintext.

Cipher text

👉 Result of encryption = unreadable gibberish.

Decryption

👉 Method by which the original meaning of Cipher text can be recovered (converting Cipher text back to Plaintext).

Open

TERMINOLOGY

CAESAR'S CIPHER

SEND TROOPS!

+3

X H Q G Y V R R S X !

A B C D E F G H I K L M N O P Q R S T V X Y Z

KEYS

Symmetric Key

👉 With Symmetric key cryptography, a single key is used for both encryption and decryption. This approach is also called “Secret Key Cryptography” since, obviously, the key must be kept secret to preserve the cipher.

Asymmetric Key

👉 Two keys are used: public and private. One key is used to encrypt the plaintext and the other is used to decrypt the cipher. It’s not important which key is used first, but sender and receiver must have both for the method to work.

KEYS

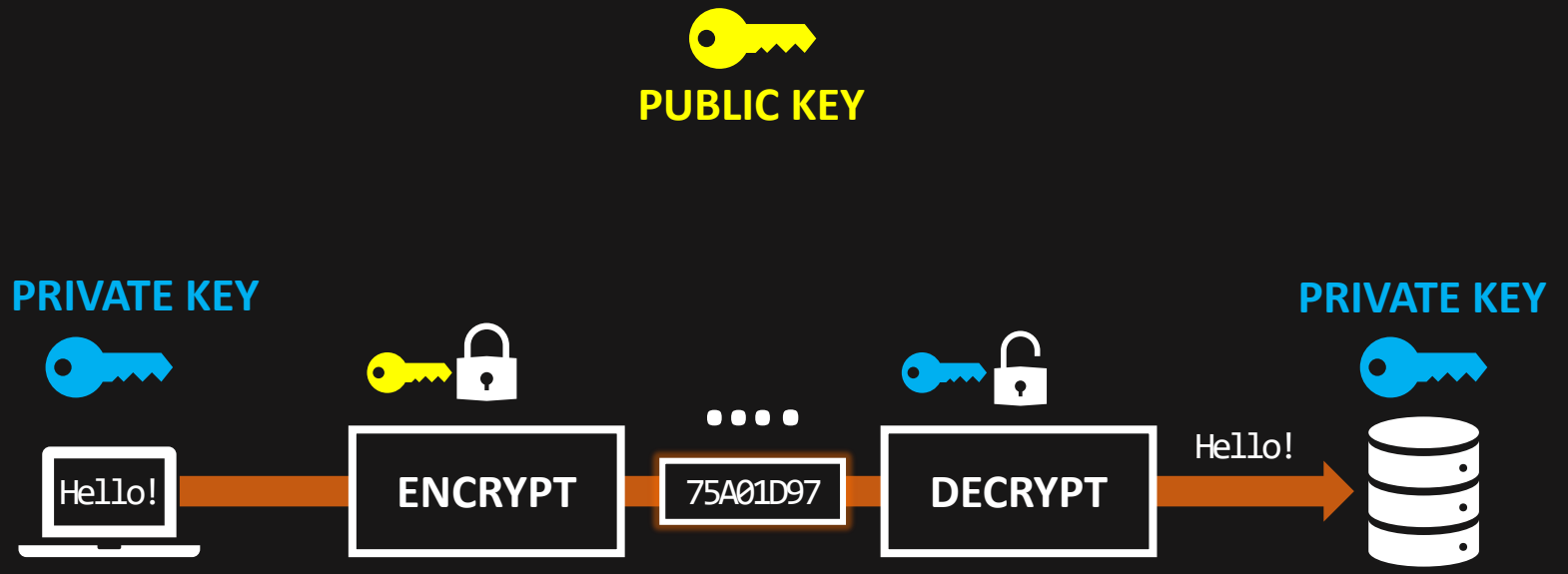
Symmetric Key

1. The same algorithm with the same key is used both for encryption and decryption
2. The key must be kept secret

Asymmetric Key

1. One algorithm is used for encryption and decryption with a pair of keys, one for encryption and one for decryption
2. One of the two keys must be kept secret

ASYMMETRIC KEYS



Open

INFORMATION SECURITY

Fundamentals