

# Confidentiality and Integrity of communications



➔ Implement a **virtual trusted channel** over an insecure medium

# Definitions

## **Plaintext**

The message in its clear form (the original message)

## **Ciphertext**

The message in its ciphered form (the encrypted message)

## **Encryption**

Transform a plaintext into ciphertext

## **Decryption**

Transform a ciphertext into a plaintext