CPR E 431

BASICS OF INFORMATION SYSTEM SECURITY

Introduction to Cryptography Tools

Video Summary

- What are Cryptography Tools
- What is Confidentiality
- How to Achieve Confidentiality
- Encryption For Confidentiality
- Attacks on Encryption Algorithms

Cryptography Tools

- Consider how many financial transactions are performed on the Internet every day. Protecting all this data is of utmost importance.

- Cryptography can be defined as the process of concealing the contents of a message from all except those who know the key.

- There are two types of cryptographic algorithms you need to know:

  ✓ Symmetric

  ✓ Asymmetric.

What is Confidentiality

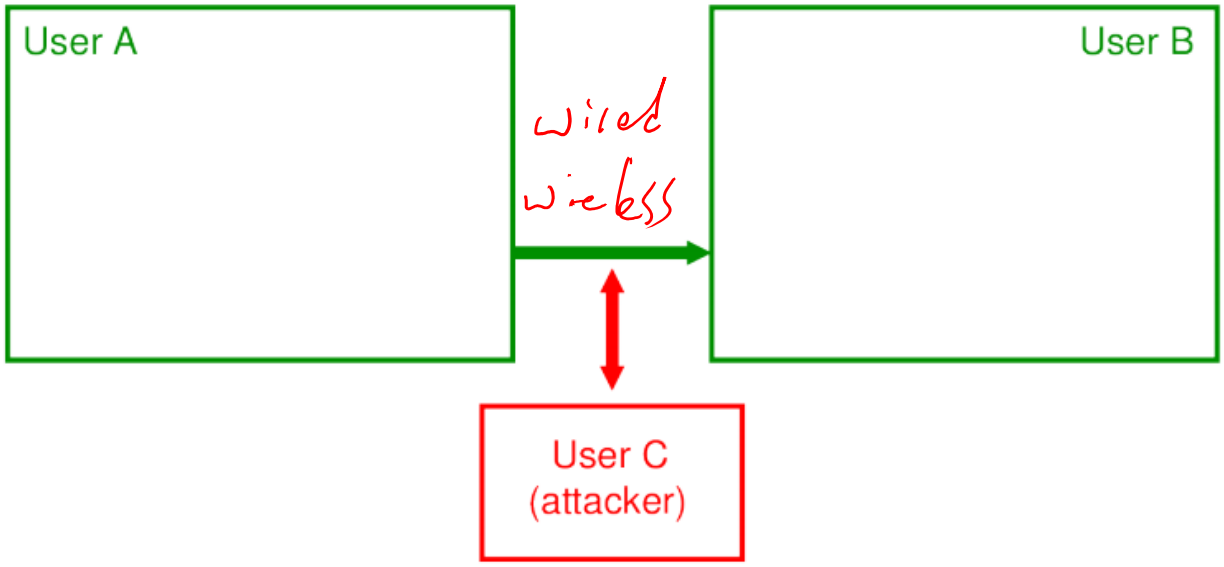
- Confidentiality simply means that what is private should stay private.
- Cryptography can provide confidentiality through the use of encryption.
- Encryption can protect the confidentiality of information in storage or in transit.
- Encryption offers an easy way to protect information

Encryption for Confidentiality

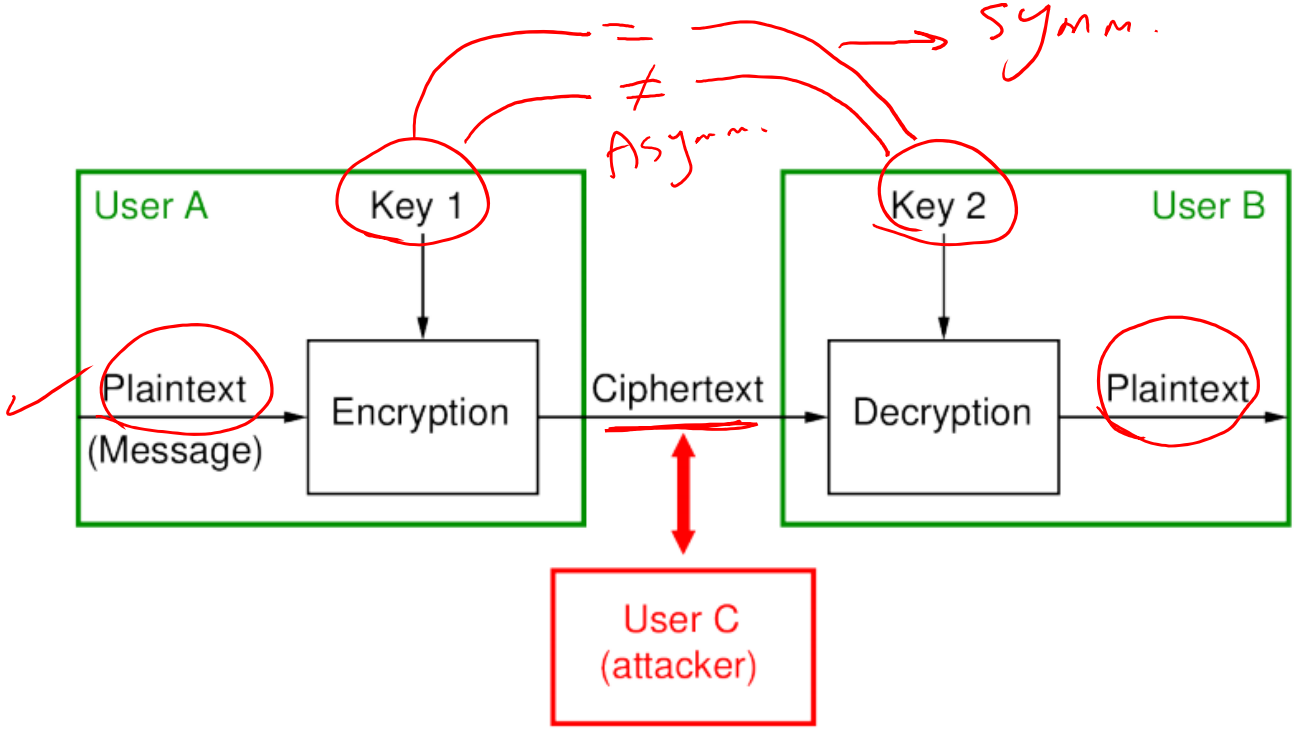
- Aim: assure confidential information not made available to unauthorized individuals (data confidentiality)

- How: encrypt the original data; anyone can see the encrypted data, but only authorized individuals can decrypt to see the original data

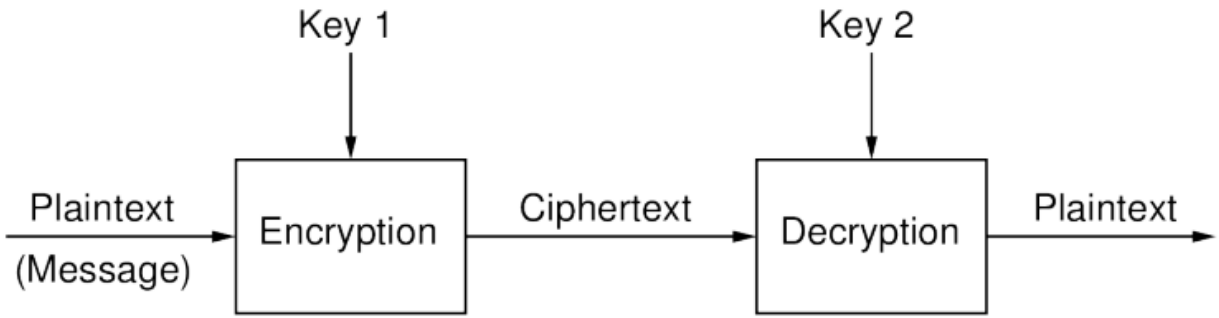
Model of Encryption for Confidentiality



Model of Encryption for Confidentiality



Model of Encryption for Confidentiality



Terminology

Plaintext	original message
Ciphertext	encrypted or coded message
Encryption	convert from plaintext to ciphertext (enciphering)
Decryption	restore the plaintext from ciphertext (deciphering)
Key	information used in cipher known only to sender/receiver
Cipher	a particular algorithm (cryptographic system)
Cryptography	study of algorithms used for encryption
Cryptanalysis	study of techniques for decryption without knowledge of plaintext
Cryptology	areas of cryptography and cryptanalysis

Requirements and Assumptions

Requirements for secure use of symmetric encryption:

1. Strong encryption algorithm: Given the algorithm and ciphertext, an attacker cannot obtain key or plaintext
2. Sender/receiver know secret key (and keep it secret)

Assumptions:

- Cipher is known
- Secure channel to distribute keys

Video Summary

- What are Cryptography Tools
- What is Confidentiality
- How to Achieve Confidentiality
- Encryption For Confidentiality
- Attacks