

## Introduction to Cryptography

Breno de Medeiros

---

---

---

---

---

---

---

## What is cryptography?

- Greek etymology:
  - kryptos: hidden
  - graphein: to write
- Algorithmic techniques to obscure the meaning of information so that it is unreadable without special knowledge.
  - Verb: Encrypt. Noun: encryption.
  - Decryption: The algorithm to recover original information from obscured source.

---

---

---

---

---

---

---

## Cryptanalysis

- The study of techniques to overcome encryption -- therefore being capable of recovering obscured information without being privy to the special knowledge.
- Cryptology: The study of both cryptography and cryptanalysis techniques
  - In this class, we shall study mostly cryptography, while learning some cryptanalytic techniques.

---

---

---

---

---

---

---

## Shared key encryption

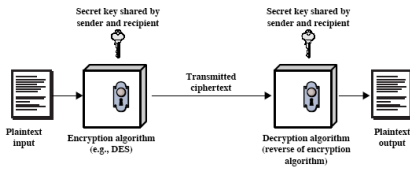


Figure 2.1 Simplified Model of Symmetric Encryption

Figure from textbook: Stallings. Cryptography and Network Security

---

---

---

---

---

---

---

---

## Terminology

- Cipher: The encryption algorithm
- Key: A secret value used by the cipher
- Plaintext: The original information before encryption is applied
- Cipher-text: The result of applying encryption to the plaintext.

---

---

---

---

---

---

---

---

## Cryptography worldview

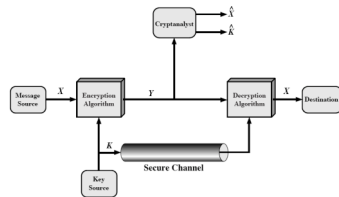


Figure 2.2 Model of Symmetric Cryptosystem

Figure from textbook: Stallings. Cryptography and Network Security

---

---

---

---

---

---

---

---

## Keys and Channels

- Knowledge of the key must be restricted only to legitimate parties.
- Key distribution channel must be secured through some means (e.g.: physical)
  - Typically: Secure channel is expensive to operate, and only limited amount of information can be conveyed that way
- Adversary (cryptanalyst) can see the transmitted cipher-text

---

---

---

---

---

---

---

---

## Other cryptographic services

- From the beginning, cryptography was used not only to conceal the meaning of messages, but also to confirm origin:
  - Only an author privy to the secret would be able to generate ciphertexts that decrypt into intelligible messages (authentication)
  - To prevent alteration of the message in transit -- editing the ciphertext results in unpredictable changes to plaintext, and detection (integrity)

---

---

---

---

---

---

---

---

## Steganography

- Steganography involves writing hidden messages in such a way that no one apart from the intended recipient knows of the existence of the message:
  - Appear as another message (cover message), or a picture.
  - Classically: invisible ink, font style changes.
  - Digitally: Insertion of information on the least significant bit of high-definition color images.

---

---

---

---

---

---

---

---