Cryptography

Lecture 1

Arkady Yerukhimovich

August 26, 2024

Outline

A (Very) Brief History of Cryptography

- For 1000s of years, cryptography was "the art of writing or solving codes"
- Largely heuristic approaches to design codes, leading to a break-fix cycle

- In the 70s and 80s, modern cryptography turned cryptography into a science, giving it a strong mathematical basis.

Principles of Modern Cryptography

- Formal definitions
- Precise assumptions
- Proofs of security

Kerckhoffs' Principle

"The cipher method must not be required to be secret, and it must be able to fall into the hands of the enemy without inconvenience."

The Rule of Modern Crypto

No security by obscurity!

Outline

Private-key encryption

Alice

Bob

Private-key encryption

Alice

Key k

Bob

Key k

Private-key encryption

Alice

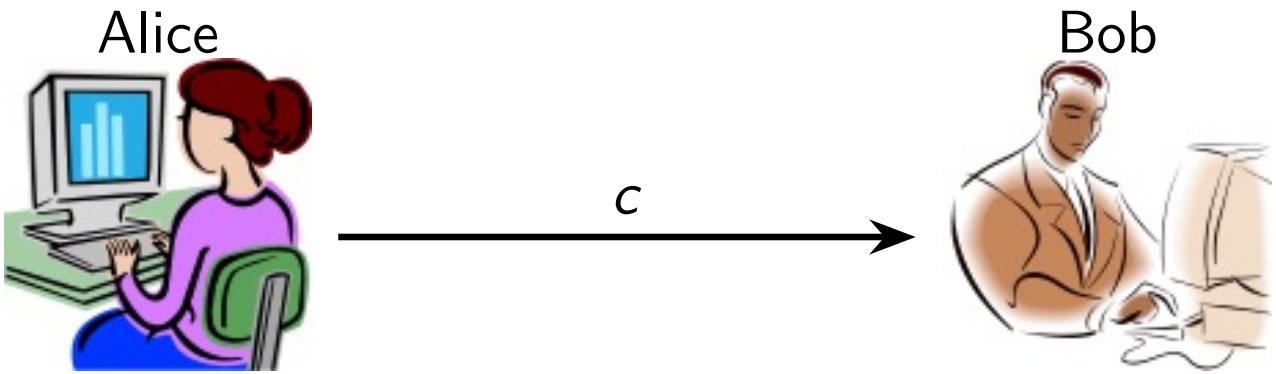
Key k

Message m

Bob

Key k

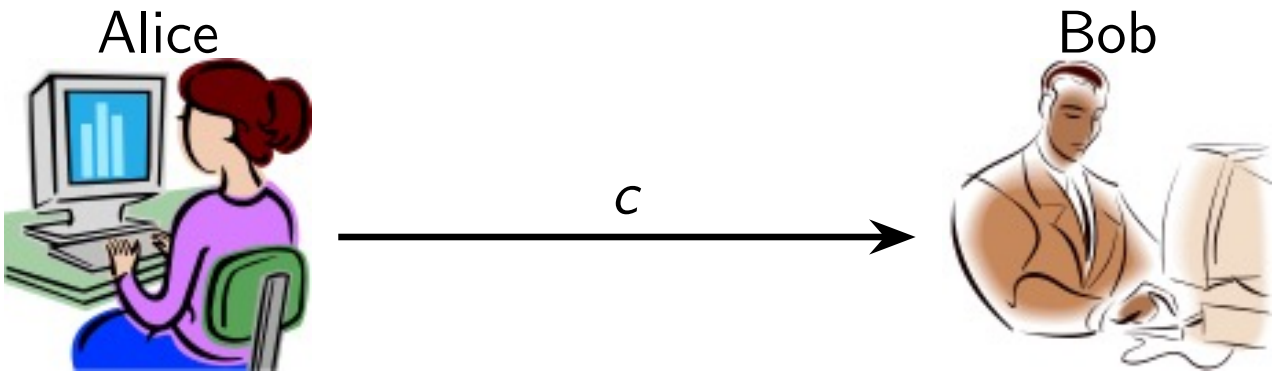
Private-key encryption



Message m

Encrypt m: $c \leftarrow \mathrm{Enc}_k(m)$

Private-key encryption



Key k
Message m
Encrypt m: $c \leftarrow \mathrm{Enc}_k(m)$

Key k
Receive ciphertext c
Decrypt c: $m = \mathrm{Dec}_k(c)$

Private-key encryption

Alice

c

Bob

Key k
Message m
Encrypt m: $c \leftarrow \mathrm{Enc}_k(m)$

Key k
Receive ciphertext c
Decrypt c: $m = \mathrm{Dec}_k(c)$

Security

Eve gets to observe c, but can not learn m

Defining Encryption Functionality

Private-key (symmetric-key) encryption scheme:

- Gen: Outputs randomly chosen key k
- $\text{Enc}(k, m) : c \leftarrow \text{Enc}_k(m)$
- $\text{Dec}(k, c) : m = \text{Dec}_k(c)$

Terminology

m - plaintext

c - ciphertext

Correctness

For all k output by Gen and all messages m, $\text{Dec}_k(\text{Enc}_k(m)) = m$

Defining Encryption Security

Security Guarantee

What is a successful attack?

Threat Model

What does the adversary know?

Defining Encryption Security

Security Guarantee

What is a successful attack?

- $\mathcal{A}$ learns the key k

Threat Model

What does the adversary know?

Defining Encryption Security

Security Guarantee

What is a successful attack?

- $\mathcal{A}$ learns the key k
- $\mathcal{A}$ learns the message m

Threat Model

What does the adversary know?

Defining Encryption Security

Security Guarantee

What is a successful attack?

- $\mathcal{A}$ learns the key k
- $\mathcal{A}$ learns the message m
- $\mathcal{A}$ learns any character of m

Threat Model

What does the adversary know?

Defining Encryption Security

Security Guarantee

What is a successful attack?

- $\mathcal{A}$ learns the key k
- $\mathcal{A}$ learns the message m
- $\mathcal{A}$ learns any character of m
- Semantic security:
  Regardless of what $\mathcal{A}$ knows about m, she learns no new information

Threat Model

What does the adversary know?

Defining Encryption Security

Security Guarantee

What is a successful attack?

- $\mathcal{A}$ learns the key k
- $\mathcal{A}$ learns the message m
- $\mathcal{A}$ learns any character of m
- Semantic security:
  Regardless of what $\mathcal{A}$ knows about m, she learns no new information

Threat Model

What does the adversary know?

- ciphertext-only

Defining Encryption Security

Security Guarantee

What is a successful attack?

- $\mathcal{A}$ learns the key k
- $\mathcal{A}$ learns the message m
- $\mathcal{A}$ learns any character of m
- Semantic security:
  Regardless of what $\mathcal{A}$ knows about m, she learns no new information

Threat Model

What does the adversary know?

- ciphertext-only
- known-plaintext

Defining Encryption Security

Security Guarantee

What is a successful attack?

- $\mathcal{A}$ learns the key k
- $\mathcal{A}$ learns the message m
- $\mathcal{A}$ learns any character of m
- Semantic security:
  Regardless of what $\mathcal{A}$ knows about m, she learns no new information

Threat Model

What does the adversary know?

- ciphertext-only
- known-plaintext
- chosen-plaintext

Defining Encryption Security

Security Guarantee

What is a successful attack?

- $\mathcal{A}$ learns the key k
- $\mathcal{A}$ learns the message m
- $\mathcal{A}$ learns any character of m
- Semantic security: Regardless of what $\mathcal{A}$ knows about m, she learns no new information

Threat Model

What does the adversary know?

- ciphertext-only
- known-plaintext
- chosen-plaintext
- chosen-ciphertext