CRYE 6127 Introduction to Cryptology

Jorge L. Villar

UBa Cyber Crypto Center, Fall 2025

Introduction

Outline

Contents

Approximate timing (14 hours in total):

- Introduction (1 hour)
- Symmetric Key Encryption (3 hours)
- Message Authentication Codes and Hashing (3 hours)
- Public Key Encryption (4 hours)
- Digital Signatures and Certificates (3 hours)

Organization

Lectures

On-line two-hours sessions with a middle short break

- **Deliverables:** Some problems to be solved (50% of the grade)
- **Final Exam** (50% of the grade)

Contact information for further assessment

By e-mail to `jorge.villar@upc.edu`

Study Material

Professor's webpage: `https://web.mat.upc.edu/jorge.villar/course_introcrypt.html`

More public resources in other sections of the same webpage

Jorge L. Villar's webpage

Home | Publications | CV | Teaching

Teaching

In the current semester (Fall 2025), I'm teaching **Probability and Statistics** for Physics Engineers and **MATLAB and Its Applications in Engineering** at ETSETB. I also teach **Data Protection** in the Master's degree in Cybersecurity (MCYBERS), at the same school .

I'm also collaborating with UBa Cyber Crypto Center and giving some on-line lectures there at the MSc level.

I have taught other subjects at ETSETB: Linear Algebra, Calculus, Advanced Calculus, Differential Equations, Mathematics for Telecommunication, Probability and Stochastic Processes and Simulation and Numerical Methods Applied to Telecommunication. In addition, I have also taught Cryptology as an optional subject at FME. I was also interested in the design of self-learning tools.

Classnotes and slides

Find below some class notes, slides and other documents related to the different subjects:

- Data Protection (Master MCYBERS)
- Cryptography (Optional subject FME)
- Introduction to Cryptology (Master Program at UBa Cyber Crypto Center)
- Security Models in Cryptography (Master Program at UBa Cyber Crypto Center)
- Codes and Cryptography (Master MAMME)
- Blockchain (PAE ETSETB)

Teaching publications

Home | Publications | CV | Teaching

Outline

Introduction

The main goal:

Efficient and Reliable Data Transmission and Storage

Introduction

The main goal:
Efficient and Reliable Data Transmission and Storage

Data: digital data source = (infinite) sequence of binary or q-ary symbols

Introduction

The main goal:
Efficient and Reliable Data Transmission and Storage

Data: digital data source = (infinite) sequence of binary or q-ary symbols

Reliable: against

- imperfect environment $\longrightarrow$ **Information Coding**
- malicious users $\longrightarrow$ **Cryptography**

Introduction

The main goal:
Efficient and Reliable Data Transmission and Storage
e.g.: Binary Data Storage

Data: digital data source = (infinite) sequence of binary or q-ary symbols

Reliable: against

- imperfect environment $\longrightarrow$ **Information Coding**
- malicious users $\longrightarrow$ **Cryptography**

Efficient: w.r.t.

- read / write / modify / delete time (per bit / per access)
- physical space
- life of stored data

Example: Binary Data Storage (I)

Reliable against imperfect environment $\longrightarrow$ **Information Coding**

Add redundancy (w/o degrading efficiency too much)

- Use error correction codes: detect/correct a few errors
- Use data shuffling: protects against correlated error locations (Compact Disk)

Example: Binary Data Storage (I)

Reliable against imperfect environment $\longrightarrow$ **Information Coding**

Add redundancy (w/o degrading efficiency too much)

- Use error correction codes: detect/correct a few errors
- Use data shuffling: protects against correlated error locations (Compact Disk)

Efficient w.r.t. physical space $\longrightarrow$ **Information Coding**

Use a compression code (w/o degrading speed too much)

Example: Binary Data Storage (II)

Reliable against malicious users $\longrightarrow$ **Cryptography**

Confidentiality: Use symmetric encryption

Integrity: Use message authentication codes

Availability: Use secret sharing schemes

The Setting (I)

Perfect environment: No storage or communication errors or excessive message delivery delays.

The Setting (I)

Perfect environment: No storage or communication errors or excessive message delivery delays.

Users: divided into

- good guys (honest)
- bad guys (corrupted by an adversary)

The Setting (I)

Perfect environment: No storage or communication errors or excessive message delivery delays.

Users: divided into

- good guys (honest)
- bad guys (corrupted by an adversary)

Alternative model: Rational Cryptography (from Game Theory). Only selfish guys (not necessarily honest, can collude).

The Setting (I)

Perfect environment: No storage or communication errors or excessive message delivery delays.

Users: divided into

- good guys (honest)
- bad guys (corrupted by an adversary)

Alternative model: Rational Cryptography (from Game Theory). Only selfish guys (not necessarily honest, can collude).

Simplest case: One honest user, one bad user.
E.g.: Secure binary data storage.

The Setting (II)

Adversarial behavior:

The Setting (II)

Adversarial behavior:

- **static:** corrupted users are fixed before starting the actual attack
- **dynamic:** corrupted users are decided on-the-fly during the attack

The Setting (II)

Adversarial behavior:

- **static:** corrupted users are fixed before starting the actual attack
- **dynamic:** corrupted users are decided on-the-fly during the attack

- **passive:** corrupted users follow the protocol and try to learn more than they are allowed to
- **active:** corrupted users deviate from the protocol in any arbitrary way

The Setting (II)

Adversarial behavior:

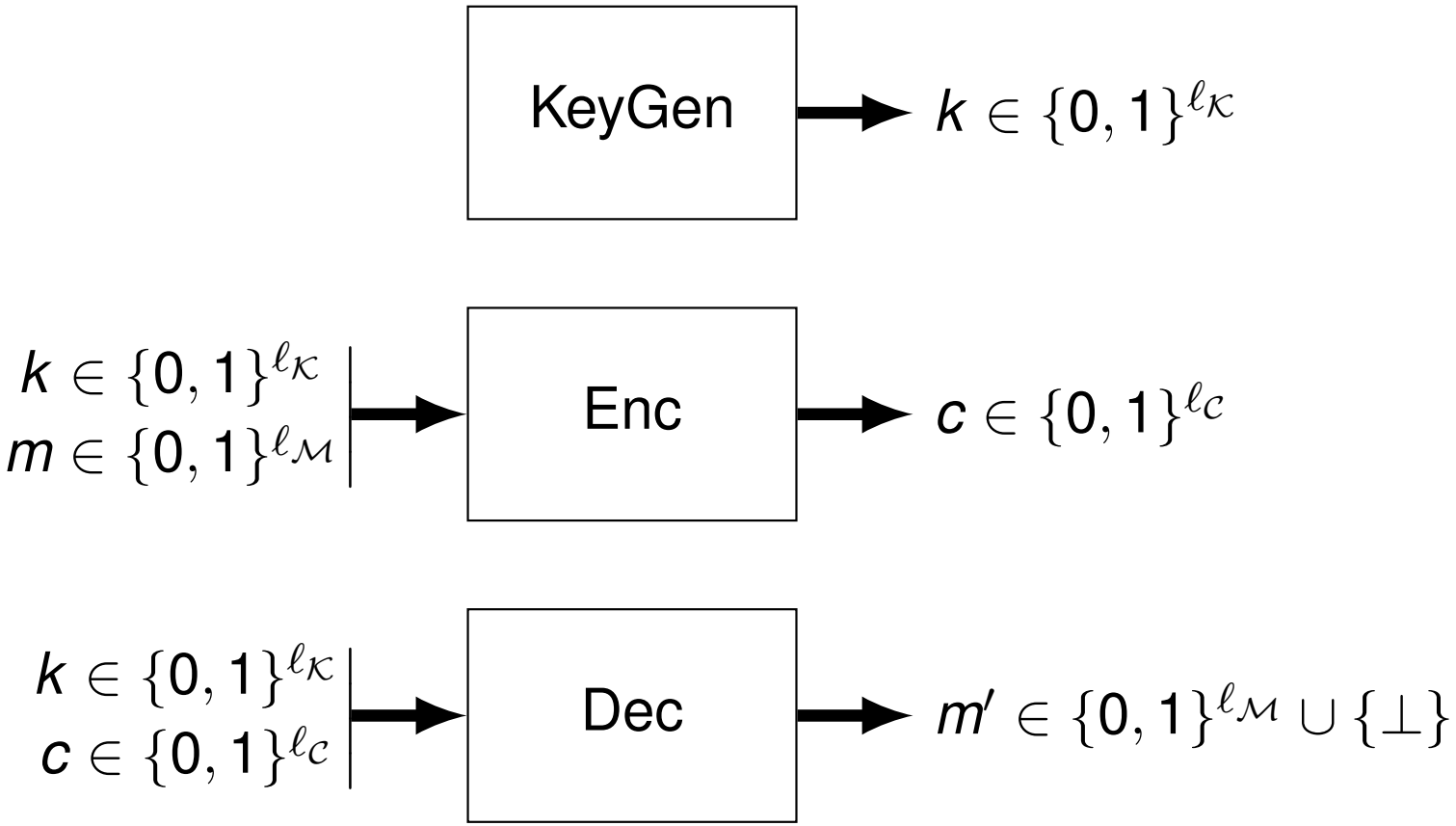
- **static:** corrupted users are fixed before starting the actual attack
- **dynamic:** corrupted users are decided on-the-fly during the attack

- **passive:** corrupted users follow the protocol and try to learn more than they are allowed to
- **active:** corrupted users deviate from the protocol in any arbitrary way

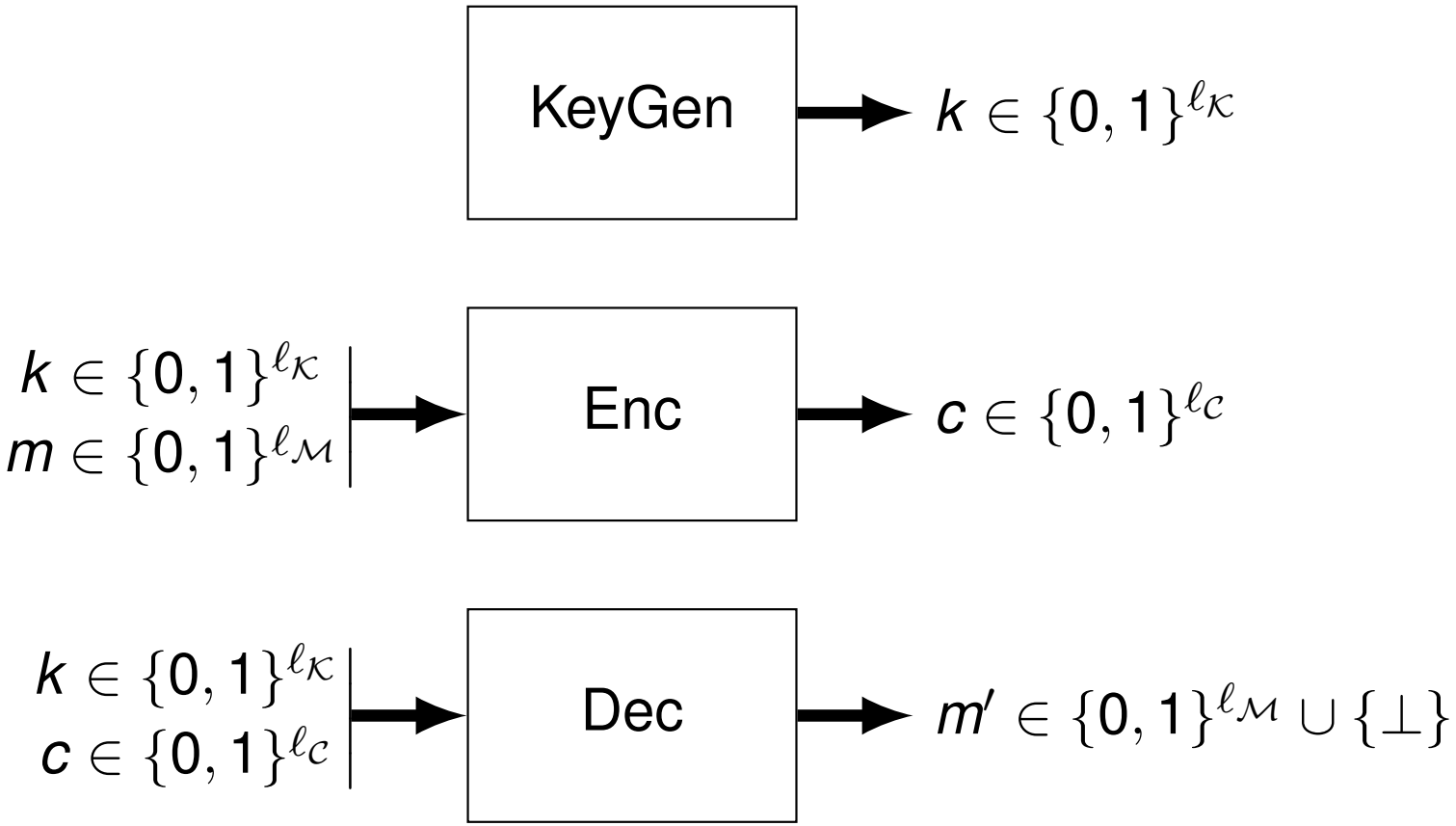
- **bounded:** the adversary has limited resources (computational power, memory)
- **unbounded:** the adversary has unlimited resources

Outline

Symmetric Key Encryption: Syntax



Symmetric Key Encryption: Correctness



$$\forall m \in \{0,1\}^{\ell_\mathcal{M}},\ \forall k \in \{0,1\}^{\ell_\mathcal{K}}, \quad m = \mathsf{Dec}(k, \mathsf{Enc}(k, m))$$

Symmetric Key Encryption: Privacy

Informal definition:

"Impossible to find m from $c = \mathrm{Enc}(k, m)$ without k".

Symmetric Key Encryption: Privacy

Informal definition:

> *"Impossible to find m from* $c = \mathrm{Enc}(k, m)$ *without k".*

More formally:

> *For any fixed* $c \in \{0,1\}^{\ell_C}$*, and for a uniformly distributed* $k \in \{0,1\}^{\ell_K}$*, the probability that* $c = \mathrm{Enc}(k, m)$ *is the same for all* $m \in \{0,1\}^{\ell_M}$*.*

Symmetric Key Encryption: Privacy

Informal definition:

> *"Impossible to find m from $c = \mathrm{Enc}(k, m)$ without k".*

More formally:

> *For any fixed $c \in \{0,1\}^{\ell_C}$, and for a uniformly distributed $k \in \{0,1\}^{\ell_K}$, the probability that $c = \mathrm{Enc}(k, m)$ is the same for all $m \in \{0,1\}^{\ell_M}$.*

Or better:

Definition (Perfect Privacy)

For any probability distribution (source) of $M \in \{0,1\}^{\ell_M}$ and for a uniformly distributed $K \in \{0,1\}^{\ell_K}$, **the random variables** M **and** $\mathrm{Enc}(K, M)$ **are independent.**

Bounds for Perfect Symmetric Key Encryption

Theorem

For any correct and perfectly private symmetric encryption scheme $\ell_{\mathcal{C}} \geq \ell_{\mathcal{M}}$ *and* $\ell_{\mathcal{K}} \geq \ell_{\mathcal{M}}$.

Proof: (A simple combinatorial argument.)

Bounds for Perfect Symmetric Key Encryption

Theorem

For any correct and perfectly private symmetric encryption scheme $\ell_{\mathcal{C}} \geq \ell_{\mathcal{M}}$ *and* $\ell_{\mathcal{K}} \geq \ell_{\mathcal{M}}$.

Proof: (A simple combinatorial argument.)

Caveat: In practice, not all binary strings in $\{0,1\}^{\ell_{\mathcal{M}}}$ are valid messages. (Use a compression code and then encrypt.)

Bounds for Perfect Symmetric Key Encryption

Theorem

For any correct and perfectly private symmetric encryption scheme $\ell_{\mathcal{C}} \geq \ell_{\mathcal{M}}$ *and* $\ell_{\mathcal{K}} \geq \ell_{\mathcal{M}}$.

Proof: (A simple combinatorial argument.)

Caveat: In practice, not all binary strings in $\{0,1\}^{\ell_{\mathcal{M}}}$ are valid messages. (Use a compression code and then encrypt.)

The key cannot be reused for further encryptions!
Enc'$(k, m_1 \| m_2) = \text{Enc}(k, m_1) \| \text{Enc}(k, m_2)$ leaks information on $m_1 \| m_2$, unless $\ell_{\mathcal{K}} \geq 2\ell_{\mathcal{M}}$.

There is no perfect solution for binary private storage!
In practice, we need $\ell_{\mathcal{K}} \ll \ell_{\mathcal{M}}$.

A Generalization for Redundant Sources

Replace the sets $\{0,1\}^{\ell_{\mathcal{M}}}$, $\{0,1\}^{\ell_{\mathcal{K}}}$, $\{0,1\}^{\ell_{\mathcal{C}}}$ by probability distributions M, K, C on some finite sets $\mathcal{M}$, $\mathcal{K}$, $\mathcal{C}$.

Replace binary length by a measure of the average information given by a random variable (Shannon's entropy).

A Generalization for Redundant Sources

Replace the sets $\{0,1\}^{\ell_{\mathcal{M}}}$, $\{0,1\}^{\ell_{\mathcal{K}}}$, $\{0,1\}^{\ell_{\mathcal{C}}}$ by probability distributions M, K, C on some finite sets $\mathcal{M}$, $\mathcal{K}$, $\mathcal{C}$.

Replace binary length by a measure of the average information given by a random variable (Shannon's entropy).

Definition (Perfect Privacy)

For any probability distribution (source) of $M \in \mathcal{M}$ and for a uniformly distributed $K \in \mathcal{K}$, **the random variables M and** $\mathrm{Enc}(K, M)$ **are independent.**

A Generalization for Redundant Sources

Replace the sets $\{0,1\}^{\ell_{\mathcal{M}}}$, $\{0,1\}^{\ell_{\mathcal{K}}}$, $\{0,1\}^{\ell_{\mathcal{C}}}$ by probability distributions M, K, C on some finite sets $\mathcal{M}$, $\mathcal{K}$, $\mathcal{C}$.

Replace binary length by a measure of the average information given by a random variable (Shannon's entropy).

Definition (Perfect Privacy)

For any probability distribution (source) of $M \in \mathcal{M}$ and for a uniformly distributed $K \in \mathcal{K}$, **the random variables M and** $\mathrm{Enc}(K, M)$ **are independent.**

Theorem (Shannon)

For any correct and perfectly private symmetric encryption scheme $H(C) \geq H(M)$ and $H(K) \geq H(M)$.

The One-Time Pad

For fixed length binary strings, $\ell_{\mathcal{M}} = \ell_{\mathcal{K}} = \ell_{\mathcal{C}} = \ell$,
$\mathsf{Enc}(k, m) = k \oplus m$ and $\mathsf{Dec}(k, c) = k \oplus c$

The One-Time Pad

For fixed length binary strings, $\ell_{\mathcal{M}} = \ell_{\mathcal{K}} = \ell_{\mathcal{C}} = \ell$,
$\mathsf{Enc}(k, m) = k \oplus m$ and $\mathsf{Dec}(k, c) = k \oplus c$

For an abelian (additive) group $\mathcal{G}$, let $\mathcal{M} = \mathcal{K} = \mathcal{C} = \mathcal{G}$,
$\mathsf{Enc}(k, m) = m + k$ and $\mathsf{Dec}(k, c) = c - k$

Perfect secrecy is guaranteed if k is uniformly distributed in $\mathcal{K}$

The One-Time Pad

For fixed length binary strings, $\ell_{\mathcal{M}} = \ell_{\mathcal{K}} = \ell_{\mathcal{C}} = \ell$,
$\mathsf{Enc}(k, m) = k \oplus m$ and $\mathsf{Dec}(k, c) = k \oplus c$

For an abelian (additive) group $\mathcal{G}$, let $\mathcal{M} = \mathcal{K} = \mathcal{C} = \mathcal{G}$,
$\mathsf{Enc}(k, m) = m + k$ and $\mathsf{Dec}(k, c) = c - k$

Perfect secrecy is guaranteed if k is uniformly distributed in $\mathcal{K}$

It is normally used as an "information theoretical" piece in more complex protocols

Weakening Secrecy

To overcome the previous limitations, consider only **computationally bounded adversaries**:

Weakening Secrecy

To overcome the previous limitations, consider only **computationally bounded adversaries**:

Definition (Perfect Privacy)

For any probability distribution (source) of $M \in \mathcal{M}$ and for a uniformly distributed $K \in \mathcal{K}$, **the random variables M and** $\text{Enc}(K, M)$ **are independent.**

Weakening Secrecy

To overcome the previous limitations, consider only **computationally bounded adversaries**:

Definition (Perfect Privacy)

For any probability distribution (source) of $M \in \mathcal{M}$ and for a uniformly distributed $K \in \mathcal{K}$, **the random variables** M **and** $\text{Enc}(K, M)$ **are independent.**

Definition (Informal Computational Privacy)

For any probability distribution (source) of $M \in \mathcal{M}$ and for a uniformly distributed $K \in \mathcal{K}$, **the random variables** M **and** $\text{Enc}(K, M)$ **behave for a bounded adversary as if they were independent.**

Weakening Secrecy

Definition (Informal Computational Privacy)

For any probability distribution (source) of $M \in \mathcal{M}$ and for a uniformly distributed $K \in \mathcal{K}$, **the random variables M and** $\text{Enc}(K, M)$ **behave for a bounded adversary as if they were independent.**

Based on efficient statistical tests a computationally bounded adversary can run.

Needs some extra assumptions from Complexity Theory.

CRYE 6127 Introduction to Cryptology

Jorge L. Villar

UBa Cyber Crypto Center, Fall 2025

Introduction

—END—