# Cryptology

Jorge L. Villar

FME, UPC, Fall 2024

## Symmetric Key Crypto

# Outline

# 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:

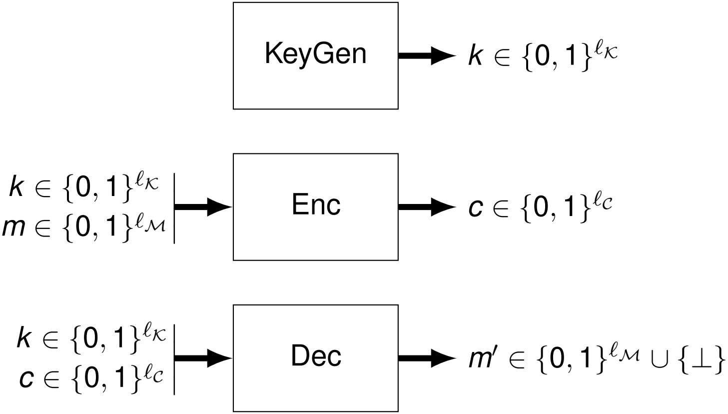
- **static:** corrupted users are fixed before starting the actual attack
- **dynamic:** corrupted users are decided on-the-fly during the attack

- **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

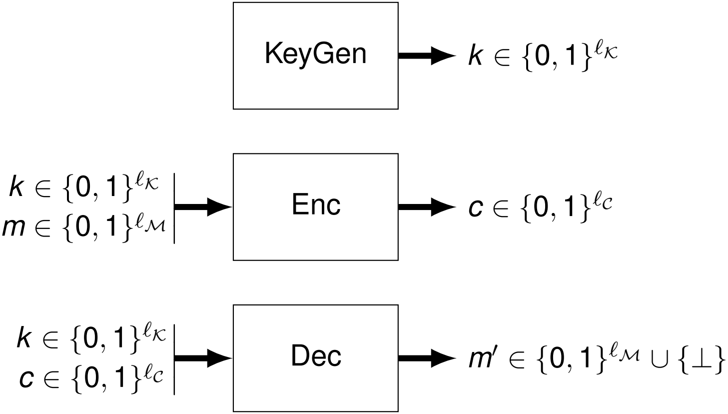
- **bounded:** the adversary has limited resources (computational power, memory)
- **unbounded:** the adversary has unlimited resources

# Outline

# Symmetric Encryption: Syntax



# Symmetric Encryption: Correctness




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

# Symmetric Encryption: Privacy

Informal definition:

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

# Symmetric Encryption: Privacy

Informal definition:

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

More formally:

*For any fixed* $c \in \{0,1\}^{\ell_{\mathcal{C}}}$*, and for a uniformly distributed* $k \in \{0,1\}^{\ell_{\mathcal{K}}}$*, the probability that* $c = \mathrm{Enc}(k, m)$ *is the same for all* $m \in \{0,1\}^{\ell_{\mathcal{M}}}$*.*

# Symmetric Encryption: Privacy

Informal definition:

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

More formally:

*For any fixed $c \in \{0,1\}^{\ell_{\mathcal{C}}}$, and for a uniformly distributed $k \in \{0,1\}^{\ell_{\mathcal{K}}}$, the probability that $c = \mathrm{Enc}(k, m)$ is the same for all $m \in \{0,1\}^{\ell_{\mathcal{M}}}$.*

Or better:

**Definition (Perfect Privacy)**

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

# Bounds for Perfect Symmetric 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 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 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, $\ell_{\mathcal{M}} = \ell_{\mathcal{K}} = \ell_{\mathcal{C}} = \ell$,
$\mathrm{Enc}(k, m) = k \oplus m$ and $\mathrm{Dec}(k, c) = k \oplus c$

# The One-Time Pad

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

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

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

# The One-Time Pad

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

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

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** $\mathrm{Enc}(K, M)$ **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** $\mathrm{Enc}(K, M)$ **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** $\mathrm{Enc}(K, M)$ **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** $\mathrm{Enc}(K, M)$ **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.

# Cryptology

Jorge L. Villar

FME, UPC, Fall 2024

END