



SAPIENZA  
UNIVERSITÀ DI ROMA

“SAPIENZA” UNIVERSITY OF ROME  
FACULTY OF INFORMATION ENGINEERING,  
INFORMATICS AND STATISTICS  
DEPARTMENT OF COMPUTER SCIENCE

---

# Cryptography

---

*Author*  
Alessio Bandiera

September 26, 2025

# Contents

<b>Information and Contacts</b>	<b>1</b>
<b>1 TODO</b>	<b>2</b>
1.1 TODO . . . . .	2

# Information and Contacts

Personal notes and summaries collected as part of the *Cryptography* course offered by the degree in Computer Science of the University of Rome "La Sapienza".

Further information and notes can be found at the following link:

<https://github.com/aflaag-notes>. Anyone can feel free to report inaccuracies, improvements or requests through the Issue system provided by GitHub itself or by contacting the author privately:

- Email: [alessio.bandiera02@gmail.com](mailto:alessio.bandiera02@gmail.com)
- LinkedIn: [Alessio Bandiera](#)

The notes are constantly being updated, so please check if the changes have already been made in the most recent version.

## Suggested prerequisites:

TODO

## Licence:

These documents are distributed under the [GNU Free Documentation License](#), a form of copyleft intended for use on a manual, textbook or other documents. Material licensed under the current version of the license can be used for any purpose, as long as the use meets certain conditions:

- All previous authors of the work must be **attributed**.
- All changes to the work must be **logged**.
- All derivative works must be **licensed under the same license**.
- The full text of the license, unmodified invariant sections as defined by the author if any, and any other added warranty disclaimers (such as a general disclaimer alerting readers that the document may not be accurate for example) and copyright notices from previous versions must be maintained.
- Technical measures such as DRM may not be used to control or obstruct distribution or editing of the document.

# 1

## TODO

### 1.1 TODO

TODO

missing  
intro-  
duction

#### Definition 1.1: Perfect secrecy

Given any distribution  $M$  over  $\mathcal{M}$ , and  $k$  chosen UAR on  $\mathcal{K}$ , we say that  $\Pi = (\text{Enc}, \text{Dec})$  is **perfectly secret** if

$$\forall m \in \mathcal{M}, c \in \mathcal{C} \quad \Pr[M = m] = \Pr[M = m \mid C = c]$$

TODO In other words, this definition requires the encrypted text  $c$  to *not reveal* anything about the plaintext  $m$ . The following lemma shows some properties about perfect secrecy.

de sta  
definizione  
non me  
torna  
la dis-  
tribuzione

#### Lemma 1.1

The following three conditions are equivalent:

1. perfect secrecy
2. independence of  $M$  and  $C$
3.  $\forall m, m' \in \mathcal{M}, c \in \mathcal{C} \quad \Pr_{k \in \mathcal{K}}[\text{enc}(k, m) = c] = \Pr_{k \in \mathcal{K}}[\text{enc}(k, m') = c]$

*Proof.* We will prove the statements cyclically.

- $1 \implies 2$ . By perfect secrecy, we have that

$$\Pr[M = m] = \Pr[M = m \mid C = c] = \frac{\Pr[M = m \wedge C = c]}{\Pr[C = c]}$$

therefore, by rearranging the terms we get that

$$\Pr[M = m \wedge C = c] = \Pr[M = m] \cdot \Pr[C = c]$$

- 2  $\implies$  3. Fix  $m \in \mathcal{M}$  and  $c \in \mathcal{C}$ ; we have that

$$\begin{aligned} \Pr_{k \in \mathcal{K}}[\text{enc}(k, m) = c] &= \Pr_{k \in \mathcal{K}}[\text{enc}(K, M) \mid M = m] \\ &= \Pr_{k \in \mathcal{K}}[C = c \mid M = m] && \text{(by definition)} \\ &= \Pr[C = c] && \text{(by independence of } M \text{ and } C) \end{aligned}$$

Now fix another message  $m' \in \mathcal{M}$ ; we can repeat the same steps and obtain that  $\Pr_{k \in \mathcal{K}}[\text{enc}(k, m') = c] = \Pr[C = c]$  which concludes the proof.

- 3  $\implies$  1. Fix  $c \in \mathcal{C}$ .

**Claim:**  $\Pr[C = c] = \Pr[C = c \mid M = m]$

*Proof of the Claim.* By assuming property 3, we get that

$$\begin{aligned} \Pr[C = c] &= \sum_{m' \in \mathcal{M}} \Pr[C = c \mid M = m'] \cdot \Pr[M = m'] && \text{(by the L.T.P.)} \\ &= \sum_{m' \in \mathcal{M}} \Pr_{k \in \mathcal{K}}[\text{enc}(k, M) = c \mid M = m'] \cdot \Pr[M = m'] \\ &= \sum_{m' \in \mathcal{M}} \Pr_{k \in \mathcal{K}}[\text{enc}(k, m') = c] \cdot \Pr[M = m'] \\ &= \sum_{m' \in \mathcal{M}} \Pr_{k \in \mathcal{K}}[\text{enc}(k, m) = c] \cdot \Pr[M = m'] && \text{(by property 3)} \\ &= \Pr_{k \in \mathcal{K}}[\text{enc}(k, m) = c] \cdot \sum_{m' \in \mathcal{M}} \Pr[M = m'] \\ &= \Pr_{k \in \mathcal{K}}[\text{enc}(k, m) = c] \\ &= \Pr_{k \in \mathcal{K}}[\text{enc}(k, M) = c \mid M = m] \\ &= \Pr_{k \in \mathcal{K}}[C = c \mid M = m] \end{aligned}$$

□

Finally, by Bayes' theorem we have that

$$\begin{aligned} \Pr[M = m] &= \frac{\Pr[M = m \mid C = c] \cdot \Pr[C = c]}{\Pr[C = c \mid M = m]} \\ &= \Pr[M = m \mid C = c] && \text{(by the claim)} \end{aligned}$$

which is precisely perfect secrecy.

□