"Sapienza" University of Rome
Faculty of Information Engineering, Informatics and Statistics
Department of Computer Science

Cryptography

Author
Alessio Bandiera

September 30, 2025

Contents

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**
- 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:

1

TODO

1.1 TODO

TODO

missing introduction

Definition 1.1: Perfect secrecy

Given any distribution M over $\mathcal{M}$, and k chosen UAR on $\mathcal{K}$, we say that $\Pi = (\mathrm{Enc}, \mathrm{Dec})$ 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 distribuzione

Lemma 1.1

The following three conditions are equivalent:

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

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

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

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

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

  $\square$

  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.

□

TODO

buco OTP