1 Objectives

The course aims to familiarize the student with the design and implementation of cryptographic primitives.

2 Program

- Classical Cryptography: algorithms and cryptanalysis.
- Shannon Theory: entropy and perfect secrecy.
- Block ciphers: DES and AES.
- Cryptographic Hash Functions and Message Authentication Codes.
- RSA and Rabin cryptosystems.
- Discrete Log-based Asymmetric Encryption.
- Digital signature schemes.

3 Evaluation

- 2 Written Tests $T_1$ and $T_2$ which contribute with the same weight to $T = (T_1 + T_2)/2$.
- 3 Individual Projects $P_1$, $P_2$ and $P_3$ involving implementation of algorithms and cryptanalysis. For graduate students, $P_3$ will be a short sequence of seminars. They contribute with the same weight to $P = (P_1 + P_2 + P_3)/3$.

The final score $M$ will be computed by the expression:

$$M = (T + P)/2.$$
For MC889, the final grade $F$ will be computed by the expression:

$$F = \begin{cases} M, & \text{se } M \geq 6 \\ (M + \text{Exam})/2, & \text{se } M \geq 2.5 \\ M, & \text{otherwise.} \end{cases}$$

Students taking the $\text{Exam}$ must satisfy a 75% attendance rate.

For MO421, the final grade $F$ will be computed by the expression:

$$F = \begin{cases} A, & \text{if } M \geq 8.5 \\ B, & \text{if } 7 \leq M < 8.5 \\ C, & \text{if } 5 \leq M < 7 \\ D, & \text{otherwise.} \end{cases}$$

Any attempt at fraud or plagiarism will be solved with $F = 0$. Attendance in class will not be evaluated for graduate students.

4 Bibliografia