INSTITUTO POLITÉCNICO NACIONAL
ESCUELA SUPERIOR DE CÓMPUTO

Cryptography

1. About the instructor

- **Name:** Sandra Díaz Santiago
- **Office:** Departamento de Ciencias e Ingeniería de la Computación.
- **email:** sds.escom@gmail.com

2. About the course

- Lectures: Monday and Thursday from 13:30 to 15:00
- Lab: Tuesday from 13:30 to 15:00
- Office hours: Wednesday from 13:30 to 15:00
  In this time you can go to my office and ask for help in the course, to solve doubts. But you can also send me an email to see you in a different hour.

2.1. Syllabus

1. Cryptography Fundamentals
2. Symmetric Cryptography
3. Public-key Cryptography
4. Digital Signatures

3. Grading

	Unit I	Unit II	Unit III	Unit IV
Presentations, reports	5 %	2 %	5 %	10 %
Homework	5 %	3 %	5 %	
Exam	-	8 %	10 %	-
Programming exercises	-	7 %	5 %	-
Project Advances	5 %	5 %	10 %	20 %
Total	10 %	25 %	35 %	30 %

- Programming exercises must be done in teams of two persons. To evaluate them you must do programs and also a written report.
- **Homeworks are a pre-requisite to have access to the lab**. You must present a hard-copy of it before the session lab starts, this hard-copy must include: your name, your group, number of homework, and date. Although you are encouraged to collaborate with your partners, you must write solutions to the homework by yourself.
- **Project.** The number of participants in a project will be 3 or 4. This number will be determined by the kind of project you choose. To check the advances of your project there will be 2 interviews, the first one at the end of unit II, and the second one at the end of unit III.

3.1. Important dates

Exam 1: September 8th (Thursday)
Exam 2: October 24th (Monday)
Complete Project: December 1st, (Thursday)

4. Textbook Information

* **Cryptography: theory and practice** by Douglas R. Stinson
* **Handbook of applied Cryptography. (Free!!)** by Alfred Menezes
* **Cryptography and Network Security** by William Stallings.
-**The Codebreakers** by David Kahn
-**The Code Book** by Simon Singh