IT security

Component
École Nationale Supérieure d'Électrotechnique d'Électronique d'Informatique d'Hydraulique et des Télécommunications

In brief

- **plugin.odf-inp:PLUGINS_ODF_COURSE_NBHOURS_TXT:** 10
- **Code:** NEGC10B

Presentation

Objectives

Introduction to basic concepts of computer systems security, in particular symmetric and asymmetric ciphering techniques, and their application to the development of authentication protocols. Introduction and illustration of discretionary and mandatory security policies, but also to intrusion tolerance techniques.

Description

The lecture is composed of four main sections:

– Introduction to basic concepts of computer security (classification of attacks, cryptography, evaluation)

– Illustration using basic examples (DES, RSA, Diffie-Hellmann, electronic signatures)

– Authentication and zero-knowledge authentication protocols (Needham-Schroeder, Fiat-Shamir, smartcards)

– Protection in computing systems (discretionary and mandatory security policies) and examples

The lecture concludes with notions of intrusion tolerance (Shamir threshold schemes, fragmentation-scattering).

Pre-requisites

Algorithmics, C / C++ programming

Useful info

Place

Toulouse