

IT Security



Component
École Nationale
Supérieure
d'Électrotechnique
d'Électronique

In brief

- > **Amety's Code:** N9EE20A
- > **Open to exchange students:** Yes

Presentation

Description

Introduction to the basic concepts of information system security (classification of attacks, cryptography, evaluation)

Illustration with examples (DES/AES, RSA, Diffie-Hellmann, electronic signatures)

Authentication and authentication protocols without knowledge sharing (Needham-Schroeder, Fiat-Shamir). Examples: Kerberos, smart cards.

Protection in computer systems (discretionary and mandatory security policies) and examples.

Concepts of intrusion tolerance (Shamir threshold schemes, etc.).

Pre-requisites

Basic knowledge of computer science (hardware, operating systems, languages).