Université Polytechnique HAUTS-DE-FRANCE

Cryptography fundamentals

ECTS
4 crédits

Composante
INSA Hauts-de-France, UPHF

Présentation

Description

Goal : Leveraging on the symmetric and asymmetric cryptographic algorithms this module will provide the main protocols and techniques implemented on existing and future networks. Last but not least, one course has been allocated for addressing network security management.

List of subjects to be presented to the students :

Introduction to modern cryptography principles
Block and stream ciphers
Groups, rings and finite fields.
The AES algorithm
Introduction to number theory: Modular arithmetics. Fermat's and Euler's Theorems. Discrete logarithms.
The Diffie-Hellman protocol
The RSA Algorithm
Elliptic Curve Cryptography
Hash functions: SHA standard
Introduction to quantum cryptography