Cryptographie

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

In brief

Code: NEIT1E

Presentation

Objectives

Apprentissage et maîtrise des aspects suivant de la cryptologie :

- Cryptographie (primitives sans clé, à clé symétrique et asymétrique)
- Cryptanalyse (attaques cryptographiques)
- Cryptographie appliquée (protocoles réseau, enclaves de sécurité, preuve de protocoles, etc.)

Description

Ce cours présente dans un premier temps les bases de la complexité pour la cryptographie et la notion d'aléa. Ensuite la cryptographie symétrique et asymétrique ainsi que les attaques habituelles sont décrites. Enfin les standards modernes et quelques notions de cryptographie avancée sont introduits. Tout ce cours alternera l'introduction aux techniques cryptographique et définitions de sécurité et notions d'attaque (qui n'ont un sens que face à des techniques cryptographiques).

A l'issue de ce cours, l'étudiant saura :

- distinguer les différents outils cryptographiques, comprendre ce qu'ils peuvent apporter à la sécurité et ce qu'ils ne peuvent pas appliquer les bonnes pratiques, et comprendre les dangers d'une utilisation inappropriée ;
- utiliser les termes techniques de la cryptographie et rechercher les propriétés qui peuvent apporter des contributions à des problèmes complexes de sécurité ;
- trouver les standards internationaux de la cryptographie, comprendre leur contenu et mettre en place une utilisation d'un outil cryptographique respectant les standards ;
- identifier les dangers classiques (homme du milieu, attaques par canaux cachés) et utiliser des modèles d'attaquant larges pour définir si une nouvelle utilisation d'un outil cryptographique est sûre ou pas