3IF1140 - Cryptographie 1

Responsables : **Jean-Francois LALANDE**

Langues d'enseignement : **FRANCAIS**

Campus où le cours est proposé : **CAMPUS DE RENNES**

Nombre d'heures d'études élèves (HEE) : **30**

Nombre d'heures présentielles d'enseignement (HPE) : **18**

Année académique : **2024-2025**

Niveau avancé : **non**

Présentation, objectifs généraux du cours :

La cryptographie est un ensemble de techniques qui permettent d'assurer des propriétés de sécurité dans un système, à savoir notamment la confidentialité des échanges, l'intégrité des messages échangés et l'authenticité des données. Ces techniques reposent sur des fondements mathématiques, mais sont mis en œuvre avec des algorithmes (primitives de chiffrement et déchiffrement par exemple) et des protocoles cryptographiques (manière de procéder à des échanges de manière sécurisée). Cette première partie de cours est dédiée aux concepts fondamentaux de la cryptographie moderne, et aux primitives cryptographiques.

Période(s) du cours (n° de séquence ou hors séquence) :

SD9

Prérequis :

- Enseignement de première année :
  - Cours SIP, cours Algorithmique, électif réseau et sécurité

Plan détaillé du cours (contenu) :

Cette première partie de 6 cours de 3h est dédiée aux concepts fondamentaux de la cryptographie moderne, et aux primitives cryptographiques :
- Introduction : concepts, principes généraux, réduction à des problèmes difficiles, modèles de sécurité
- Chiffrement symétrique (par flot et par bloc) : RC4, DES, 3DES, AES
- Chiffrement asymétrique : RSA, El Gamal, courbes elliptiques
- Intégrité symétrique, Fonctions de hachage
- Signature
- Quantique et Cryptographie

Déroulement, organisation du cours :

Cours magistraux (18h)

Moyens :

Enseignants :

- Didier ALQUIE.

Acquis d'apprentissage visés dans le cours :

A la fin de cet enseignement, l'étudiant sera capable de :

- Evaluer les propriétés des différentes primitives cryptographiques,
- Utiliser les différentes primitives cryptographiques en fonction des propriétés de sécurité attendues.

Description des compétences acquises à l'issue du cours :

C2.1 - Thoroughly master a domain or discipline based on the fundamental sciences or the engineering sciences.

Bibliographie :

- Oded Goldreich. Foundations of Cryptography (2 volumes)
- N. Fergusson, B. Schneier. Cryptographie : Sécurité de l’information et des systèmes.