3IF5030 - Cryptographie 2

Responsables : **Jean-Francois LALANDE**

Langues d'enseignement : **FRANCAIS**

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

Nombre d'heures d'études élèves (HEE) : **35**

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 seconde partie de cours est dédiée aux protocoles cryptographiques, et aux attaques par canaux auxiliaires.

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

SM10

Prérequis :

- Enseignement de première année :
  - Cours SIP, cours Algorithmique, électif réseau et sécurité
- Enseignement de 3A :
  - Crypto 1

Plan détaillé du cours (contenu) :

- Cours 1 (3h) - Protocoles cryptographiques : authentification, échanges de clé, canal sécurisé
- Cours 2 (3h) - Exemple de protocoles cryptographiques : Diffie-Helmann, TLS, IPSEC ...
- TP 1 (3h) - Déploiement de TLS
- TP 2 (3h) - Déploiement de IPSEC.
- Cours 3 (3h) - Attaques par canaux auxiliaires.
- TP 3 (3h) - Attaques par analyse de consommation de courant.

Déroulement, organisation du cours :

Cours magistraux (9h) et travaux pratiques (9h)

Organisation de l'évaluation :

Evaluation des comptes rendus de TP.

Moyens :

Enseignants :

- Ronan LASHERMES (Inria)

Acquis d'apprentissage visés dans le cours :

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

- Analyser des protocoles cryptographiques afin de s'assurer qu'ils assurent les propriétés de sécurité voulues,
- Utiliser les protocoles cryptographiques adéquates pour assurer les propriétés de sécurité voulues,
- Appréhender les risques liés aux attaques par canaux auxiliaires.

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.