Cryptographie et sécurité			12X014
			Eduardo SOLANA (CC)
Nombre d'heures par semaine	cours exercices pratique	2 2	Semestre d'automne ☒ Semestre de printemps Total d'heures 56

Cursus	Type	Crédits ECTS
Bachelor en sciences informatiques	Obligatoire	5

OBJECTIFS :

Ce cours a pour sujet l'étude et l'analyse de la sécurité des systèmes informatiques en mettant l'accent sur les aspects cryptographiques.

Sur le plan de la cryptographie, on aborde des questions qui se rapportent à des schémas de cryptage, à des générateurs pseudos-aléatoires et à des signatures digitales. On traite également les protocoles d'authentification et d'établissement de clés ainsi que les questions relatives à l'identité digitale et à la certification. Le cours aborde également les aspects technologiques des monnaies virtuelles et de la blockchain.

CONTENU :

- Bases mathématiques et modèles de calcul
- Schémas de chiffrement et de signature digitale
- Protocoles d'authentification et d'établissement de clés
- Identité digitale et certification

Bibliographie :

- **Handbook of Applied Cryptography**. Menezes, A et al. CRC series on discrete mathematics and its applications. 1997.
- **Cryptanalysis of Number Theoretic Ciphers**. Samuel S. Wagstaff, Jr. Computational Mathematic Series. Chapman & Hall /CRC, 2003.
- **Cryptography Theory and Practice. (4th Edition).** Douglas R. Stinson and Maura B. Paterson Chapman & Hall /CRC Press 2019.
- **Cryptography and Network Security: Principles and Practice (8th Edition).** Williams Stallings.Pearson, 2020.

Forme de l'enseignement	Cours et exercices intégrés
Documentation	Support de cours et liste d'ouvrages de référence
Préalable requis	Connaissances de base en informatique théorique
Préparation pour	-
Mode d'évaluation	Ecrit
Sessions d'examens	JF/AS