Mission à l'Ecole Doctorale (EDST) de l'Université Libanaise du 16 au 23 Février 2019

Par Safwan El Assad (Polytech Nantes)

Formation doctorale de 12 H, niveau Doctorat et Master 2 sur :
La sécurité des données classique et la sécurité basée chaos

Objectif du cours :

- Connaître les enjeux de la sécurité des données et les services essentiels associés

- Connaître et savoir mettre en œuvre (conception et réalisation), d'algorithmes de chiffrement basés chaos et des fonctions de hachage pour la protection des données (services : confidentialité des communications et intégrité des données).

Plan :

- Introduction et généralités sur la cryptographie classique et celle basée chaos. Etude de l'algorithme (Standard) AES.
- Chiffrement par flux et par bloc basé chaos. Dans chaque type de chiffrement nous présentons de façon détaillée deux cryptosystèmes conçus et réalisés dans notre laboratoire.
- Travail collaboratif impliquant toute la classe: aide, discussion et évaluation du travail réalisé par binôme sur une étude de cas, article de recherche sur un cryptosystème donné, à analyser, synthétiser puis présenter sous forme de Power point.