Module CHIFFR

Objectifs pédagogiques

A la fin du module, l'étudiant sera capable de:

- choisir et déployer la bonne technologie de chiffrement et de signature électronique en fonction des vulnérabilités connues et potentielles
- mettre en place une infrastructure à clé publique (PKI) et une authentification EAP
- améliorer la performance embarquée à l'aide d'accélérateurs matériels

Prérequis

- notions de logarithme, exponentielle, de calcul algébrique, polynomial et matriciel

Contenu

- chiffrement moderne en profondeur : théorie et pratiques
  - AES, DES, polynômes de Galois, Diffie-Hellman, RSA, génération de clés, types d'attaque
  - fonctions de hâchage
  - générateurs aléatoires
- authentification ; chemins et réseaux de confiance
- application sur plateformes Microsoft, Linux, mobile et embarquées

Formes d'enseignement

- 50% exposé et exercices théoriques
- 50% pratique

Evaluation

- questionnaire théorique

Organisation

Crédits ECTS	2
Périodes	30 (6 soirs)
Lieu	Neuchâtel
Responsable de module	Ninoslav Marina
Intervenant(s)	Ninoslav Marina, Marc Schaefer, Michaël Müller, Claudio Cortinovis, André Liechti
Dates	selon planification