Descriptif de module

Domaine : Haute Ecole Arc Ingénierie

1. Intitulé de module Principe et application moderne du chiffrement (CHIFFR)

Type de formation : ☐ Bachelor ☐ Master ☐ MAS ☐ DAS ☒ CAS ☐ Autres :

Langue principale d'enseignement : ☒ Français ☐ Anglais ☐ Allemand

2. Organisation

Crédits ECTS : **2**

Périodes **: 30** (6 soirs)

Volume de travail :

	heures
Enseignement	22.5
Travail personnel	37.5
Travail total	60

3. Prérequis

☐ Avoir validé le module
☐ Avoir suivi le module
☐ Pas de prérequis
☒ Autres : notions de logarithme, exponentielle, de calcul algébrique, polynomial et matriciel

4. Compétences visées / Objectifs généraux d'apprentissage

Compétences visées par le module	**A l'issue du module, l'étudiant est 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.

5. Modalités d'évaluation et de validation

Evaluation des apprentissages

- Evaluations des différentes Unités d'Enseignement (UE)

Note finale du module :

M = moyenne des notes obtenues (au dixième de point).

Conditions de réussite :

Note finale du module M ≥ 4.0 (arrondie au demi-point)
Moyennes

La note finale du module permet d'établir la note ECTS.

6. Modalités de remédiation

☒ Remédiation possible
☐ Pas de remédiation
☐ Autre (précisez) : …

6a. Modalités de remédiation (en cas de répétition)

☒ Remédiation possible
☐ Pas de remédiation
☐ Autre (précisez) : …

7. Contenu et formes d'enseignement

Module	**CHIFFR**	
Méthode d'enseignement	- 50 % Exposé et exercices théoriques - 50 % pratique	
Modalités d'évaluation	Questionnaire théorique	
Description du contenu (mots clés)	**Chiffrement moderne en profondeur : théorie et pratique** - 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**	
Supports de cours	Au choix de l'enseignant	
Outils utilisés	Au choix de l'enseignant	
Bibliographie	Communiqué par l'enseignant	
Particularité d'organisation	Lieu Responsable de module Intervenant(s) Dates	Neuchâtel Ninoslav Marina Ninoslav Marina, Marc Schaefer, Claudio Cortinovis, André Liechti Selon planification