Introduction à la Cryptographie

TEM1003-NAIN_

Domaine : **Sciences** Grade académique : **Master en architecture des systèmes informatiques - Namur**
Niveau de certification : **7** Cycle : **Deuxième cycle** Année académique : **2026-2027** (Q1)

CRÉDITS ECTS	VOLUME HORAIRE
5	**60 h**
PRÉREQUIS	**CO-REQUIS**
Aucun	*Aucun*

IMPLANTATION	DIRECTEUR DE DÉPARTEMENT DU DOMAINE	RESPONSABLE DE L'UE	ENSEIGNANTS INTERVENANTS
Département technique de Namur	Willem Kuypers	Florentin Rochet	Florentin Rochet

PROGRAMME D'ÉTUDES

Programme	Bloc	Caractère
IE-Master en architecture des systèmes informatiques	1	Obligatoire

Partie 1 Contribution de l'UE au profil d'enseignement du programme et acquis d'apprentissage spécifiques (AAS) sanctionnés par l'évaluation

CONTEXTUALISATION

UE prérequise : aucune

Cette UE contribue à l'atteinte des acquis d'apprentissage terminaux suivants :

• Agir de façon réflexive et autonome, en équipe, en partenariat

– Organiser son temps, respecter les délais

– Acquérir une capacité d'autocritique

– Actualiser ses connaissances et compétences

– Collaborer activement avec d'autres

– Animer et accompagner une équipe

– Assumer les responsabilités associées aux actes posés

• Utiliser des procédures et des outils

– Exploiter les outils appropriés afin de résoudre une tâche spécifique

– Effectuer des tests, des contrôles et des mesures

– Effectuer des paramétrages, des réglages

ACQUIS D'APPRENTISSAGE SPÉCIFIQUES (AAS)

A la fin du cours, l'étudiant.e aura progressé dans sa capacité à comprendre le fonctionnement et la garantie de la Cryptographie pour la confection de systèmes sécurisés.

• L'étudiant.e pourra décrire et modéliser un adversaire.

• L'étudiant.e pourra discuter les propriétés de sécurité des principales primitives en Cryptographie.

• L'étudiant.e pourra décrire de façon rigoureuse des notions de sécurité découlant des propriétés des principales primitives en Cryptographie.

• L'étudiant.e pourra mettre en oeuvre ces apprentissages dans un contexte de sécurisation des communications numériques.

OBJECTIFS DE DÉVELOPPEMENT DURABLE

Document annexe à la fiche UE accessible via un lien explicitant en quoi le programme d'études s'inscrit dans une politique de développement durable. Une ou plusieurs UE spécifique(s) pourraient être ciblée(s) dans cette annexe.

Partie 2 Description de l'unité d'enseignement

OBJECTIFS

À définir

CONTENU

Théorie et Laboratoires

• Rappels de notion de probabilités et de notions réseaux.

• Notions de chiffrement, définitions et progression des définitions pour assurer une résistance à un adversaire possédant de plus en plus de capacités.

• Modélisation d'attaquant

• Chiffrement symétrique : depuis l'abstraction élémentaire vers des constructions concrètes et leurs modes : AES, Chacha. Stream ciphers & Block ciphers.

• Intégrité des communications : authentification des messages sur base de clé secrète et fonctions de hachage.

• Cryptographie asymétrique : Diffie-Hellman, techniques d'échange de clé sur base de groupes algébriques.

SOURCES ET RÉFÉRENCES

À définir

SUPPORTS DE COURS

Activité d'apprentissage	Support
AAIN1003-A — Théorie	*À définir*
AAIN1003-B — Laboratoires	*À définir*

Partie 3 Méthodologie mise en œuvre et éventuel découpage de l'UE

DESCRIPTION DES ACTIVITÉS D'APPRENTISSAGE (AA) AU REGARD DE LEUR STATUT

Activité d'apprentissage	Heures	Langue d'enseignement	Langue d'évaluation
AAIN1003-A — Théorie	30 h	Français	Français
AAIN1003-B — Laboratoires	30 h	Français	Français

MÉTHODES D'ENSEIGNEMENT ET D'APPRENTISSAGE

Activité d'apprentissage	Méthodes d'enseignement et d'apprentissage
AAIN1003-A — Théorie	*À définir*
AAIN1003-B — Laboratoires	*À définir*

DÉTERMINATION DE LA COHÉRENCE PÉDAGOGIQUE EN CAS DE REGROUPEMENT D'AA FAISANT L'OBJET D'UNE ÉVALUATION DISTINCTE

À définir

Partie 4 Évaluation de l'unité d'enseignement

STRUCTURE DU DISPOSITIF GÉNÉRAL D'ÉVALUATION (EN LIEN AVEC LE PROGRAMME D'ÉTUDES)

Évaluation intégrée : non

UE remédiable.

Évaluation : session de janvier (Q1) et seconde session (Q3).

Note de l'UE : moyenne pondérée des notes des activités d'apprentissage :

• AAIN1003-A – Théorie : 50 %

• AAIN1003-B – Laboratoires : 50 %

MÉTHODOLOGIE DE CONSTRUCTION DE LA NOTE FINALE DE L'UE

Se référer à l'évaluation des activités d'apprentissage.

LA PONDÉRATION DE L'ÉVALUATION DE L'UE À DES FINS DE DÉLIBÉRATION LORS DU CALCUL DE LA MOYENNE

Au sein du programme d'études, lors du calcul de la moyenne, la pondération de l'évaluation de l'unité d'enseignement est effectuée sur base des crédits affectés à cette unité d'enseignement et évalués

MODALITÉS D'ÉVALUATION PAR ACTIVITÉ D'APPRENTISSAGE

Activité d'apprentissage	Modalités d'évaluation
AAIN1003-A — Théorie	*À définir*
AAIN1003-B — Laboratoires	*À définir*

MODALITÉS CONCRÈTES D'ÉVALUATION

Une mention sur la fiche informera les étudiants du fait que les précisions sur les épreuves seront disponibles sur Moodle au plus tard 6 semaines avant l'évaluation.