Module : Cryptographie				Code	
				ING-4-SSIR-S7-P1	
Période	**Semestre1**	*Volume horaire*	**42**	*ECTS*	**4**

Responsable	**Souheib Yousfi**	*email*	souheib.youssfi@gmail.com
Equipe pédagogique	Souheib yousfi, Mohamed Basti Mahjoubi		

1. Objectifs de Module *(Savoirs, aptitudes et compétences)*

Ce module porte sur les notions de base de la sécurité informatique en s'appuyant sur les concepts de la cryptographie.

Acquis d'apprentissage :

A la fin de cet enseignement, l'élève sera capable de :

- Maîtriser les primitives cryptographiques. (**C1.2**)
- Caractériser les chiffrements symétriques et asymétriques. (**C1.2**)
- Simuler et tester en s'appuyant sur des outils cryptographiques. (**C1.3**)
- Concevoir une infrastructure à clé publique. (**C1.1**)
- Communiquer un serveur avec des clients en s'appuyant sur openssl. (**C3.3**)

Compétences
C1.2 Appliquer les connaissances théoriques de la cryptographie dans des travaux pratiques.
C1.3 Une maitrise des commandes Linux pour bien simuler et pratiquer la cryptographie.
C1.4 Maitrise des sockets clients serveur.
C3.2 Concevoir et modéliser des solutions garantissant les primitives cryptographiques.

2. Pré-requis*(autres UE et compétences indispensables pour suivre l'UE concernée)*

- Les commandes LPIC1 et LPIC2
- La programmation Python
- Les communications client serveur
- Réseaux

3. Répartition d'Horaire de Module

Intitulé de l'élément d'enseignement	*Total*	*Cours*	*TD*	*Atelier*	*PR*

Module :…Cryptographie……..	42h	27h	3h	12h	

4. Méthodes pédagogiques et moyens spécifiques au Module
(pédagogie d'enseignement, ouvrages de références, outils matériels et logiciels)

- Supports de Cours
- Projecteur et Tableau
- Travaux dirigés
- Logiciels de simulation : openssl

Bibliographie

Titre	Auteur(s)	Edition
Les notions de la cryptographie	D.Chaum	2004
Les primitives cryptographiques	A. Enderson	2015

5. Contenu *(Descriptifs et plans des cours / Déroulement / Détail de l'évaluation de l'activité pratique)*	Durée allouée	
Module 1 : Cryptographie		
Séance 1 • Les notions de base de la cryptographie	Cours	3H
Séance 2 • Les chiffrements Symétriques	Cours	3H
Séance 3 • Application des chiffrement symétriques	TP	3H
Séance 4 • Les chiffrement Asymétriques..	Cours	3H
Séance 5 • Application des chiffrement asymétriques.	TP	3H
Séance 6 • Les fonctions de hachage	Cours	3H
Séance 7 • Assurer l'intégrité avec les fonctions de hachage	TP	3H
Séance 8 • Les infrastructures à clés publiques .	TP	3H

Séance 9 • Les certificats électroniques	Cours	3H
Séance 10 • Gestion des clés publiques et sécurisation d'accès à un site web	TP	3H
Séance 11 • Virtualisation d'accès avec VPN.	TP	3H
Séance 12 • Le protocoles AES	Cours	3H
Séance 13 • Le protocole RSA	Cours	3H
Séance 14 • Le protocole Elgamal	Cours	3h

6. Mode d'évaluation de Module*(nombre, types et pondération des contrôles)*

Eléments d'enseignement	Coeff	DS	EX	TP	PR
Module - Cryptographie	2	40%	60%		

Pour valider le module, les étudiants passeront un examen dont le coefficient est de 60%, un DS dont le coefficient est de 40% .

La durée de tous les examens (Examen, DS…) est de 1h30.

Le DS est planifié 7 semaines après le début du module et portera sur les thématiques suivantes :

- Les notions de base de la cryptographie
- Les chiffrement Symétriques
- Les chiffrement asymétriques
- Le hachage

Quand à l'examen, il est planifié après l'écoulement des 14 semaines et portera sur toutes les thématiques enseignées tout au long des 42 heures.

Le module est validé si l'étudiant obtient une moyenne supérieure ou égal à 10 sur 20.