Cryptographie

Domaine Ingénierie et Architecture
Filière Informatique et systèmes de communication
Orientation Sécurité informatique (ISCS)
Mode de formation Temps partiel/En emploi

Informations générales

Nom : Cryptographie
Identifiant : CRY
Année académique : 2021-2022
Responsable : Alexandre Duc
Charge de travail : 150 heures d'études
Périodes encadrées : 96 (= 72 heures)

Semestre	E1	S1	S2	E2	S3	S4	E3	S5	S6	E4	S7	S8
Cours									48			
Laboratoire									48			

Connaissances préalables recommandées

L'étudiant-e doit connaître et savoir utiliser les notions suivantes :

- mathématiques d'ingénieurs ;
- bases de la sécurité informatique ;
- bases de la programmation procédurale.

Les unités d'enseignement MAT1, MAD, MAT2, MAT3, ISI, PRG1 et PRG2 permettent d'acquérir ces connaissances.

Objectifs

À la fin de ce cours, l'étudiant sera capable de

- connaître un bref aperçu de l'histoire de la cryptographie et en nommer les jalons essentiels ;
- expliquer l'importance de la cryptographie lors de certains grands événements historiques ;
- expliquer les raisons du développement fulgurant de la cryptographie moderne dans le monde civil ;
- connaître le vocabulaire essentiel utile en cryptographie et l'appliquer à bon escient ;
- expliquer la notion d'aversaire ainsi que leur typologie ;
- expliquer le principe de Kerckhoffs et ses enseignements ;
- posséder une vue synoptique des différents types d'algorithmes cryptographiques et de leurs buts ;
- expliquer et appliquer le concepts de division euclidienne et de divisibilité sur les entiers ;
- expliquer et appliquer les concepts de nombre premier, de plus grand diviseur commun, de factorisation unique d'un nombre entier, et de répartition des nombres premiers ;
- expliquer et appliquer le crible d'Eratosthène, l'algorithme d'Euclide pour calculer un PGCD ainsi que l'algorithme d'Euclide étendu pour calculer l'identité de Bézout ;
- expliquer les concept de groupe, de groupe cyclique, d'ordre d'un élément et de générateur ;
- énoncer et appliquer les théorèmes de Fermat-Euler, de Lagrange et des restes chinois ;
- expliquer le concept d'anneau et de corps fini ;
- expliquer et appliquer l'arithmétique sur l'anneau des polynômes sur un corps ;
- expliquer la construction du corps de Galois GF(p^n) ;

- expliquer le fonctionnement d'un algorithme de chiffrement linéaire et expliquer comment le casser ;
- expliquer la notion d'algorithme de chiffrement par flot et celle d'algorithme de chiffrement par bloc ;
- expliquer le fonctionnement du masque jetable, ainsi que sa sécurité, et en donner ses limites pratiques ;
- connaître les caractéristiques principales des algorithmes de chiffrement symétriques les plus utilisés ;
- connaître, expliquer le fonctionnement et donner les limites des modes opératoires les plus utilisés ;
- énumérer les propriétés et expliquer le fonctionnement d'une fonction de hachage; citer le nom de fonctions de hachage sûres ;
- expliquer le domaine d'application des MAC ainsi que le fonctionnement et les limites de HMAC et de CBC-MAC ;
- expliquer les différents types de protocoles d'authentification symétriques, ainsi que leurs propriétés sécuritaires ;
- expliquer le fonctionnement et les aspects sécuritaires du protocole de Diffie-Hellman ;
- expliquer le fonctionnement et les aspects sécuritaires du chiffrement RSA et El Gamal ;
- expliquer le fonctionnement et les aspects sécuritaires des signatures RSA et DSA ;
- expliquer la démarche menant au choix de la taille de clefs cryptographiques pour des algorithmes symétriques et asymétriques ;
- décrire et expliquer la méthode de génération de grands nombres premiers reposant sur le test de Miller-Rabin ;
- expliquer et appliquer l'algorithme d'exponentiation rapide de type «square-and-multiply» ;
- expliquer les principes derrière le groupe des points d'une courbe elliptique, ainsi que la loi d'addition de points ;
- appliquer le théorème de Hasse, ainsi que le calcul du nombre de points d'une courbe elliptique définie sur une extension de corps ;
- expliquer le fonctionnement du protocole de Diffie-Hellman ainsi que le chiffrement d'El Gamal lorsqu'implémenté sur le groupe des points d'une courbe elliptique ;
- expliquer le concept d'infrastructure à clefs publiques, ainsi que les notions sous-jacentes ;
- donner un aperçu du protocole SSL/TLS, de son utilisation ainsi que de son fonctionnement interne ;
- utiliser les langages de programmation Python et Sage pour coder des modules cryptographiques simples.

Contenu et formes d'enseignement

Répartition des périodes indiquée à titre informatif.

Cours: 48 périodes

- Introduction et histoire de la cryptographie	3
- Terminologie et types d'adversaires	3
- Théorie des nombres	3
- Groupes finis	3
- Anneaux et corps finis	6
- Algorithmes de chiffrement symétriques	6
- Authentification symétrique	3
- Chiffrement à clef publique	6
- Signatures digitales	3
- Courbes elliptiques	3
- Cryptographie pratique	3
- PKI et SSL/TLS	6

Laboratoire: 48 périodes

- Exercices pratiques en classe	24
- Cryptanalyse classique	6
- Cryptographie symétrique	6
- Cryptographie à clef publique	6
- PKI et SSL/TLS	6

Bibliographie

Douglas Stinson, "Cryptographie: théorie et pratique", Vuibert, 2003.

Contrôle de connaissances

Cours : l'acquisition des matières de cet enseignement sera contrôlée au fur et à mesure par des tests et des travaux personnels tout au long de son déroulement. Il y aura au moins 2 tests d'une durée totale d'au moins 3 périodes.

Laboratoire : ils seront évalués sur la base des rapports de manipulation, à 3 reprises au minimum.

Examen : L'atteinte de l'ensemble des objectifs de formation sera vérifiée lors d'un contrôle final commun écrit d'une durée de 120 minutes.

Matériel autorisé :
- Information communiquée directement par l'enseignant.

Calcul de la note finale

Note finale = moyenne cours x 0.3 + moyenne laboratoire x 0.2 + moyenne examen x 0.5