Cryptologie

Objectifs

Les objectifs de ce cours sont de découvrir les principes de chiffrement symétrique, asymétrique et de hachage.

Mathématiquement nous nous attarderons sur l'algorithme d'Euclide étendu pour son application dans le processus de construction des clefs (privées) du chiffrement RSA.

Informatiquement, au delà de quelques algorithmes de chiffrement symétrique élémentaire, nous explorerons des bibliothèques dédiée au chiffrement et au hachage en python.

Cours

Un cours très détaillé est disponible ici.

`www.ataraxy.info/Crypto`

Ce cours est très (trop) complet est permettra aux étudiants curieux à en apprendre plus. Son axe principal sont les mathématiques mais compte tenu du volume attribué, nous explorerons de manière superficiel cette dimension.

Support

Pour ce cours, vous disposez :
- d'une fiche résumé qu'il vous appartient de la compléter en prise de note
- d'une feuille de TD
- d'un notebook jupyter contenant tous les TP (assurez-vous que les bibliothèque `cryptography` et `hashlib` soient installées)

Organisation du cours

Un bloc représente une séance d'une heure et demi

Bloc	Nature	Programme
1	CTD	Crypter
2	CTD	Hasher
3	CTD	Chiffrement symétrique
4	TP	Petits algorithmes de chiffrement
5	TP	Bibliothèque `cryptography`
6	TP	Bibliothèque `haslib`
7	CTD	Le protocole RSA (I)
8	CTD	Le protocole RSA (II)
9	TP	Le protocole RSA en pratique
10	EX	Évaluation

Evaluations

Évaluation continue : (coef. 1) participation, TP, savoir-être.

Évaluation finale : (coef. 3)
- Savoir réaliser un (dé)chiffrement symétrique vu en cours
- Savoir restituer le mécanisme du protocole RSA (clefs et principe)
- Avoir de la *culture cryptographique* (législation, hashage vs cryptage, grand théorèmes ...)