Cryptologie

Objectifs

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

Mathématiquement nous nous attarderons sur le calcul modulaire, l'algorithme d'Euclide étendu, les matrice modulaires et la recherche de leur inverse.

Informatiquement, nous utiliserons la langage python pour instancier les différents cryptosystèmes que nous introduirons.

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.

Support

Pour ce cours vous disposez, en ligne de l'intégralité du cours, des exercices, des exercices générés aléatoirement et auto-corrigés ainsi que des différents notebook vous assistant dans la réalisation des TP.

Organisation du cours

Un bloc représente une séance d'une heure et demi

Bloc	Nature	Programme
1	C	Le calcul modulaire : chiffrement de César
2	TD	Chiffrement de César : exercices
3	TP	Chiffrement de César
4	TP	Attaque : brute force
5	C + E	L'inverse modulaire : chiffrement affine
6	TD	Chiffrement de affine : exercices
7	TP	Chiffrement de affine
8	TP	Attaque : fréquentielle
9	CTD + E	Chiffrement de Vigénère
10	TP	Attaque : Kasiski

Bloc	Nature	Programme
11	C	Matrice modulaire : chiffrement de Hill
12	TD	Chiffrement de Hill : exercices
13	TP	Chiffrement de Hill
14	TP	Attaque : claire connu
15	C + E	Vers RSA : histoires cryptologiques
16	C	Vers RSA : les mystérieux nombres premiers
17	TD	RSA : exercices
18	TP	Tests de primalité
19	TP	RSA : chiffrement et clefs
20	E	Évaluation

Evaluations

Évaluation continue : chiffrement symétrique

- Calcul modulaire et chiffrement de César (séance 5 - coef. 1)
- Inverse modulaire et chiffrement affine (séance 9 - coef. 2)
- Matrice modulaire et chiffrement de Hill (séance 15 - coef. 3)

Évaluation finale : chiffrement asymétrique (coef. 5)

- 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, grands théorèmes ...)