Cergy, le 15 décembre 2016

ENSEA-Cergy 95 Département Signal et Télécommunications (http://www.ensea.fr/)

Stage LIESSE : Cryptologie avec Python

Date : 4 séances sur deux journées, mercredi 10 et jeudi 11 mai 2017

Objectif du stage :

Présentation de systèmes cryptologiques anciens et modernes et des outils mathématiques associés.
Applications à divers contextes.
Étude des attaques possibles. Mise en œuvre avec Python 3 du cryptage et décryptage.
Des notions élémentaires de Python sont nécessaires, mais suffisantes.
Chaque séance comprendra une partie de travaux personnels sur machine avec Python 3, avec des outils de démonstration donnés, et leurs utilisations pour résoudre les exercices.
On utilisera son portable personnel avec Python 3 et les bibliothèques standards.
Quelques portables de l'école pourront être prêtés en cas de nécessité.
Il est souhaitable d'avoir installé une version de Python 3, avec par exemple Anaconda 3.
Déjeuner organisé à proximité de l'ENSEA.

10 mai, 9 h -12 h P.David : Ex-enseignant de mathématiques à l'ENSEA

1- 1.1 Historique des codes classiques. Principe de Kerckhoffs.

1.2 Cryptologie classique (codes linéaires,Vigenere, Hill) et leurs faiblesses.

1.3 Attaque des codes classiques. Statistiques lexicales, indice de concordance.

1.4 Présentation de l'AES. Les différents concepts mathématiques de l'AES : Corps GF(256), polynômes sur ce corps, et leurs implémentations par des classes en Python.

1.5 AES en Python.

10 mai, 13 h 30 -17 h Ph. Bouafia: Enseignant de mathématiques à l'ENSEA

2- 2.1 Méthode de chiffrement symétrique : le DES.
2.2 Attaque du double DES.
2.3 Cryptanalayse différentielle du DES à 3 tours.

11 mai, 9 h -12 h P.David : Ex-enseignant de mathématiques à l'ENSEA

3- 3.1 Outils de théorie des nombres : primalité, factorisation, arithmétique modulaire,

Fractions continues, Théorème du reste chinois. Test de primalité de Miller-Rabin.

3.2 Systèmes à clé publique : RSA, variantes, contextes d'utilisation

3.2 Faiblesses du RSA, conditions de mise en oeuvre efficace.

3.3 Exemple d'attaques du RSA : attaques de Fermat, de Wiener, de Wiener étendue.

3.4 Le domaine de sécurité du RSA.

11 mai, 13 h 30 -16 h30 Ph. Bouafia: Enseignant de mathématiques à l'ENSEA

4- Fonctions de condensation (hachage).

4.1 Notion de sécurité pour les fonctions de hachage.

4.2 Algorithme de Chaum-Van Heijst-Pfitzmann.

4.3 Recherche de collisions, attaque des anniversaires avec une table de hachage.

4.4 Cassage de mots de passe.

16 h 30 -17 h Bilan du stage

Contact à l'ENSEA : Ph Bouafia et P. David Département Signal et Télécommunications
Tél: 01-30-73-66-66 Courriels : philippe.bouafia@ensea.fr et david@ensea.fr
École Nationale Supérieure de l'Électronique et de ses Applications
6 Avenue du Ponceau 95000 Cergy