Télécharger des documents locaux
CRYPTOGRAPHIE : Les fiches de cours de A. Cruptos

Fiches de niveau 0

fichecrypto_000.pdf Introduction à la cryptologie moderne (V2 - Mai 2010)

fichecrypto_001.pdf La division euclidienne (V2 - Mai 2010)

fichecrypto_002.pdf L'algorithme de Horner (V2 - Mai 2010)

fichecrypto_003.pdf Opérations de base modulo n (V2 - Mai 2010)

fichecrypto_004.pdf Calculer une puissance modulo n

Fiches de niveau 1

fichecrypto_100.pdf Preuve par invariant de boucle

fichecrypto_101.pdf Arithmétique de base - Le pgcd et le ppcm

fichecrypto_102.pdf Le théorème de Bézout

fichecrypto_103.pdf Le théorème des restes chinois

fichecrypto_104.pdf La fonction d'Euler

fichecrypto_105.pdf Calcul de l'inverse modulo n

fichecrypto_106.pdf Le petit théorème de Fermat et ses généralisations

fichecrypto_107.pdf Eléments primitifs de Z/pZ (p premier)

fichecrypto_108.pdf Le problème du logarithme discret dans Z/pZ

fichecrypto_109.pdf Les conversions classiques entre types de données

fichecrypto_110.pdf La primitive RSA

fichecrypto_111.pdf Construction de nombre premiers

fichecrypto_112.pdf Complexité de l'algorithme d'Euclide étendu

Fiches de niveau 2

fichecrypto_200.pdf Les résidus quadratiques

fichecrypto_201.pdf Les fractions continues

fichecrypto_202.pdf Chiffrer avec RSA

fichecrypto_203.pdf Chiffrement mixte

fichecrypto_204.pdf Attaque de RSA par fractions continues

fichecrypto_205.pdf Echange de clé de Diffie-Hellman

fichecrypto_206.pdf Quelques primitives cryptographiques

fichecrypto_207.pdf Statistiques sur le PGCD de nombres au hasard (V2 - Mai 2010)

fichecrypto_208.pdf Algorithme de Montgomery pour la multiplication modulaire (V2 - Mai 2010)

fichecrypto_209.pdf Attaque par faute de la signature RSA

fichecrypto_210.pdf Extraire une racine carrée modulo n

fichecrypto_211.pdf Chiffrement à clé secrète par blocs en mode CBC

fichecrypto_212.pdf Chiffrement à clé secrète par blocs en mode Galois Counter

Fiches de niveau 3

fichecrypto_300.pdf La sécurité parfaite de Claude Shannon

fichecrypto_302.pdf Forme de la biclé RSA générée par OpenSSL

CRYPTOGRAPHIE : Cours, Présentations
Formation générale en cryptographie

fgc.pdf Le cours sous forme de présentation

annexe_1.pdf Fonctionnement d'AES

annexe_2.pdf Algorithmes arithmétiques classiques

annexe_3.pdf Cryptographie à clé secrète

annexe_4.pdf Les modes d'utilisation

annexe_5.pdf Algorithmes classiques

annexe_6.pdf Clé publique

complexite.pdf complexite des algorithmes

Cours Ecole de Cryptographie d'Oujda 2009

Techniques cryptographiques

primitives_crypto.pdf Primitives cryptographiques

Corps finis, courbes elliptiques

crypto_cf.pdf Cryptographie et corps finis, une présentation

crypto_el.pdf Cryptographie et courbes elliptiques, initiation

annexe_1.pdf Le corps fini à 16 éléments

annexe_2.pdf Liens entre éléments générateurs

annexe_3.pdf Quelques résultats de dénombrements

annexe_4.pdf Exemple d'éléments normaux et de polynômes normaux

annexe_5.pdf Les 30 polynômes irréductibles de dégré 8 sur F_2

annexe_6.pdf addition sur une courbe elliptique

annexe_7.pdf Quelles courbes elliptiques?

Protocoles et standards cryptographiques
GNUpg

gnupg_armure.pdf l'armure ascii de gnupg, radix64

gnupg_revoque.pdf Comment révoquer une clé gpg

Openssl

openssl_1.pdf Notes sur OpenSSL : Partie I

openssl_2.pdf Notes sur OpenSSL : Partie II

OpenSSL-fichiers-cnf.zip Fichiers de configuration utilisés par openssl

Générateurs pseudo-aléatoires

Sécurité des générateurs pseudo-aléatoire (théorème de Yao)

Sécurité du générateur de Blum Blum Shub. Partie I

CRYPTOGRAPHIE : Exercices
Exercices d' arithmétique

X_arith_Rec.pdf Exercices d'arithmétique pour la cryptographie

CRYPTOGRAPHIE : ARCANA-ECDB.

Une base de données de courbes elliptiques bonnes pour la cryptographie classique (signature ECDSA, échange de clé ECDH) ainsi qu'une base de courbes d'Edwards

ARCANA-ECDB

Rapport technique sur la construction de cette base de courbes.

CRYPTOGRAPHIE : Les démonstrations logicielles de A. Cruptos
Kruptor, le paquetage en xcas
de démonstrations de crypto

Kruptor est un paquetage de procédures écrites en xcas dans le style Maple, qui permet de programmer facilement des démonstrations des fonctionnements des systèmes cryptographiques. La nouvelle version (version 2016) a été réécrite pour s'adapter à la version en vigueur de xcas (version 1.1.1-12)

Attention : ces composants ont été développés sous linux et testés sous linux. Quelques essais rapides ont été faits sous windows vista, mais il se pourrait que quelques fonctions ne marchent pas tout à fait bien.

Kruptor 2.1.tgz

CRYPTOGRAPHIE : Les implémentations

Implémentation d'AES (limité aux clés de 128 bits) sur un microcontroleur pic 16F876, fournie par Pascal Véron (Université de Toulon-Var).

rijndael.asm