Introduction à la Cryptographie

Eléments pour le projet

Cécile Pierrot

Supports de E. Thomé

Telecom Nancy, 2A ISS – 2021

Plan

Introduction

Objectif du projet

Principe : le projet est un jeu à scénario.

- Je suis un décideur pressé ;
- Je veux une fiche descriptive [1] (1 page recto-verso maxi, soit 6000 à 10000 signes) sur un sujet donné.
- Grosso modo, je veux des éléments de réponse sur ≪est-ce que j'achète cette technologie≫, et pourquoi.

Je fixe un ensemble de sujets possibles.

Projet à réaliser seul ou en binôme. Les groupes de 3 ne sont pas acceptés.

1. Google Image : "fact sheet" pour avoir une idée du rendu.

Sujets proposés

- Les modes opératoires ≪modernes≫ comme GCM ;
- La cryptanalyse différentielle ;
- Les attaques sur le DES ;
- Le cryptosystème Blowfish ;
- L'aléa dans le noyau Linux avec /dev/random, et les alternatives Windows et MacOS ;
- Les atouts et difficultés du chiffrement symétrique et asymétrique sur Android (processeur ARM 32 bits) ;
- Les atouts et difficultés du chiffrement symétrique et asymétrique sur Iphone ;
- Dual-EC-DRBG et les manipulations de standards ;

Sujets proposés

- “Safe curves”, et le IRTF CFRG ;
- La difficulté du logarithme discret dans les corps finis ;
- La difficulté du logarithme discret sur les courbes elliptiques et hyperelliptiques ;
- La cryptanalyse dans Millenium IV, et plus précisément : la difficulté de la factorisation d’entiers, et les tailles de clés RSA rencontrées dans divers contextes ;
- Les attaques sur MD5, SHA-0, SHA-1 ;
- Les menaces sur SHA-2 et SHA-256 ? ;
- Keccak/SHA-3 ;
- TLS v1.3 : Protocole, preuves et attaques ;
- La cryptographie à base de réseaux euclidiens ;
- Les menaces de l’ordinateur quantique sur la cryptographie.

Sujets proposés

- La cryptographie dans le contexte du vote électronique ;
- La cryptographie à base de couplages ;
- Le chiffrement homomorphe ;
- La cryptographie pour le cloud ;
- Les systèmes de chiffrement de disque dur ;
- Les systèmes de chiffrement et de signature de mail ;
- La cryptographie dans les documents d'identité ;
- Le protocole EMV et ses faiblesses ;
- Les protocoles SSH, et IKE (d'un point de vue cryptographie) ;
- Le crible quadratique (NFS) ;
- Les attaques par canaux cachés ;
- L'utilisation des FPGA pour la cryptanalyse ;

Qu'est-ce qui m'intéresse ?

Ça dépend des cas, mais les choses suivantes peuvent être intéressantes.

- Objectifs de la technologie ;
- Fonctionnement ;
- Historique, articles fondateurs, articles très en vue ;
- Actualité chaude de la thématique ;
- Performances soft/hard ;
- Coûts de déploiement ;
- Logiciels existants et leurs perfs, tableaux de bench comparatifs ; Support système (win/mac/linux/android/ios) ;
- Avantages/inconvénients ;
- Les menaces en terme d'attaque du protocole ;
- Longévité ?
- Qui je dois recruter sur cette techno ?

Sources de documentation

Il est permis de regarder Wikipedia. Le copier/coller est en revanche idiot, c'est la première chose que je vérifierai. Les articles de cryptographie sont disponibles en ligne par exemple sur `eprint.iacr.org`.

Attention, votre fiche doit refléter la situation d'aujourd'hui !

Calendrier :

- Pour mardi 23 mars : je veux savoir qui traite quoi ; Vous m'envoyez un message privé sur Teams avec : le nom éventuel de votre binôme. Votre sujet préféré + votre sujet de secours. Premier arrivé, premier servi.
- Projet à rendre pour le mercredi 26 mai, heure de votre choix. Par mail à cecile.pierrot@inria.fr . Soutenance le 28 mai.

La fiche compte pour 2/10 de la note. Le Quizz (28 mai) pour 3/10. L'oral compte pour 5/10 : oral de 15 minutes + 5 minutes de questions.