Projet : Cryptographie pour le futur

Conception et analyse de protocoles cryptographiques

L'objectif de ce projet est d'apprendre à concevoir des protocoles cryptographiques et à analyser leur sécurité.

Il conviendra de définir une solution théorique, qui inclura la déscription des techniques utilisées et l'analyse de sécurité de la solution proposée. De plus, il faudra identifier les menaces et problèmes potentiels ayant trait à la solution proposée, aucune solution n'étant parfaite.

Attention : L'originalité sera apreciée ! Aucune solution ressemblant à des protocoles existants de nos jours ne sera notée.

1 Instructions générales

Le projet est à réaliser par groupe de (maximum) 3 étudiants. La solution devra être rendue au plus tard le 1er avril sous la forme suivante :

1. **Un texte** éventuellement assorti de graphiques et références, d'une longueur maximale de 8 pages A4 (à envoyer par courriel au format PDF à l'enseignant).
   Votre texte doit être rédigé avec soin et présenter une réelle synthèse du travail effectué – préciser les techniques utilisées et une analyse détaillée de la solution trouvée. Il comporte trois parties : Introduction, Contenu et Conclusions comme precisé dans la déscription.
2. **Une présentation** orale de 10 minutes effectuée en classe, à l'aide de diapositives (5-10 diapositives environ à soutenir le 4 avril).
3. ***Optionnel*** : en fonction du projet, à votre choix, une brève démonstration en classe de la implémentation des solutions envisagées (sur vos machines).

2 Notation – 40 pts

La note du projet tiendra compte des aspects suivants :

1. **Conception [10 pts] :** compréhension du sujet, bonne utilisation des principes cryptographiques étudiés, qualité et justification des solutions données, exactitude des techniques employées, etc.
2. **Originalité de la solution [10 pts] :** le travail doit être original, les sources utilisées seront citées, il est interdit de proposer des protocoles existants, deux projets évidemment similaires ne seront pas pris en compte.
3. **Texte [10 pts] :** qualité de la synthèse, clarté du document, présentation des solutions, pertinence et complétude de l'analyse de sécurité, etc.

anca.nitulescu@ens.fr

4. **Oral [5 pts] :** organisation et clarté de la présentation, préparation de diapositives, choix et pertinence des exemples, interactivité, etc.
5. **Travail de groupe [5 pts] :** organisation de l'équipe, précision dans la division des taches, chacun des étudiants d'un groupe doit être capable de délimiter clairement sa contribution.
6. **Bonus [+3 pts] :** pour le meilleur projet – le groupe avec la solution la plus originale.

*Les troix premiers points sont, bien entendu, les plus importants Si une solution demande une analyse substantielle, celle-ci est prise en compte dans l'évaluation de la conception du sujet.

La profondeur du travail réalisé compte pour environ la moitié des points Conception et Texte. Un projet parfait mais minimal, sans grande difficulté qui donne une solution triviale et une analyse très facile, ne récoltera qu'une note moyenne. Inversement, un travail qui propose une solution complexe, verra sa note augmentée.

3 Description

L'an 2100 : Le commencement d'une nouvelle ère cryptographique.
Vous êtes dans le futur. Les domaines de l'informathique ont connu des progrès surprenants dans les dernieres décennies. Touts les schémas cryptographiques du passé sont cassés (ceux de l 'an 2016 inclus). C 'est dans vos mains de rétablir la sécurité de la communication de votre temps.

• Introduction

Présentez les nécessités de votre monde, le besoin de la crypto dans la vie des gens, la protection souhaitée et les buts à atteindre.

Précisez les menaces et leurs occurrences dans votre scénario du futur et étudiez les moyens de lutter contre toutes les attaques possibles.
Votre solution doit garantir :
— la confidentialité des données,
— l'authenticité (authentification et identification),
— l'intégrité des données.

Utilisez votre imagination ! Vous devez vous placer dans le contexte de votre monde fictif.
Décrivez votre monde et ses innovations :
— Precisez les machines existantes,
— Les technologies de la comunication,
— Les puissances de calcul actuelles,
— Les nouveaux outils mathématiques.

*Utilisez des outils mathématiques existants dans le passé - algèbre modulaire, nombres réels, géométrie, etc.
Ou inventez des nouvelles structures logiques, des conventions ou des formules de calcul en donnant leur définition et en décrivant leur fonctionnement.

Attention !

Les principes de la cryptographie restent les mêmes. On utilisera les notions apprises en cours.

4 Passez au travail !

Proposez des schémas et des primitives cryptographiques pour atteindre les exigences de sécurité souhaités :
— un schéma de chiffrement à cle publique,
— un schéma de signature,
— une fonction de hachage.
Étudiez la sécurité et les vulnérabilités de vos solutions. La structure à suivre est la suivante :

• Contenu

1. Définir (au moins) un problème difficile et justifier pourquoi ce n'est pas possible de le résoudre efficacement avec les moyens de vôtre temps.
   Baser la sécurité de vos protocoles sur ce(s) problème(s).
2. Pour les protocoles proposés, le cryptosystème et le schéma de signature :
   (a) Décrire les algorithmes correspondants.
   (b) Justifier pourquoi ça marche ?
   Vos algorithmes sont pertinents, les définitions sont réspectées et le déchiffrement ou la vérification fonctionnent.
   (c) Quelle sont les propriétés particulières de vos shémas ?
   Chiffrement déterministe, propriétés homomorphes, malléabilité, etc.
3. Présenter les adversaires de votre époque. Analyser leur buts et leur moyens.
4. Faire une analyse de sécurité :
   (a) Presenter les différents niveaux de sécurité classifiés par but-moyens de l'adversaire
   (b) Mentionner les niveaux atteints
   (c) Faire des preuves de réduction de sécurité en utilisant le(s) problème(s) difficile(s).
   (d) Identifier les vulnérabilités : les niveaux de securité qui ne sont pas atteints par vos schémas.
   (e) Illustrer des attaques possibles si la sécurité n 'est pas parfaite.

• Conclusions

Décrivez les progrès de votre monde fictif après avoir apporté cette innovation cryptographique. Mentionnez les problèmes qui restent ouverts.

Définissez le rôle de chacun dans votre groupe de travail : l'organisation de l'équipe, la division des taches, les contributions de chacun.

Résumez le processus de travail : les objectifs fixés au début, le déroulement des différentes étapes, les difficultés que vous avez éprouvés, comment vous avez réfléchi pour arriver à chaque construction, les résultats obtenus par rapport à vos attentes initiales, vos impressions sur le travail, etc.

- Bibliografie :

- **Intro to RSA Encryption** (ou la crypto expliquée avec des couleurs)
  https://www.youtube.com/watch?v=dleUxfghd5I
- **Cryptographie à clé publique** (Exo7 : Vidéos de l'Université de Lille)
  https://www.youtube.com/watch?v=6KfJXl-Kvws
- **Introduction à la cryptographie**
  ftp://ftp.pgpi.org/pub/pgp/6.5/docs/french/IntroToCrypto.pdf
- **PICSI :** Parcours Fonctions de hachage et intégrité
  http://www.picsi.org/parcours_40.html
- **PICSI :** Parcours Signatures électroniques
  http://www.picsi.org/parcours_69.html
- **Handbook of Applied Cryptography** de A. Menezes, P. van Oorschot, and S. Vanstone.(CRC Press, Boca Raton, Florida, October 1997)
  http://www.cacr.math.uwaterloo.ca/hac/
- **Ars Cryptographica**
  http://www.apprendre-en-ligne.net/crypto/menu/index.html
- **Cryptographie Paris 13**
  https://www.math.univ-paris13.fr/~boyer/enseignement/PolyCrypto2010.pdf
- **La Science du secret** de Jacques Stern (Odile Jacob, 1998)
- **A Course in Computational Number Theory** de H. Cohen. (Springer-Verlag, 4th edition, 2000)
- **La Guerre des Codes Secrets : des Hiéroglyphes à l'Ordinateur** de D. Kahn. (Inter Editions, 1st edition, 1980)
- **Applied Cryptography** de B. Schneier. (John Wiley Sons, 2nd edition, 1996)
  Traduction en français de Marc Vauclair.