PLAN DE COURS
Été 2024

UQAC

8INF874 • Cryptographie

Enseignant :
Courriel :

Description sommaire

Des algorithmes de cryptographie (DES, AES, RSA, …) à la complexité des chiffrements en passant par la cryptanalyse, les protocoles cryptographiques, les propriétés usuelles de sécurité, ce cours gradué est l'occasion de comprendre le fonctionnement, les forces, les limites ainsi que les applications des systèmes cryptographiques classiques et modernes. Ce cours traite de la cryptographie d'un point de vue essentiellement théorique et n'abordera pas la sécurité informatique comme telle. Ce cours s'adresse aux étudiants avec une bonne connaissance des mathématiques discrètes. Toutefois, cette condition ne devrait pas empêcher l'étudiant intéressé de s'inscrire puisqu'un rappel des notions mathématiques importantes sera effectué en début de trimestre.

Objectifs du cours

Voici quelques objectifs visés par ce cours :

- Connaître les différents systèmes de chiffrement principaux classiques et modernes (DES,AES, RSA, ElGamal, courbes elliptiques, etc.) et être en mesure d'expliquer leurs fondements.
- Être en mesure d'identifier les différentes applications de la cryptographie dans la vie courante.
- Identifier quelques problèmes d'ingénierie provoqués par l'implantation, le déploiement et l'utilisation d'algorithmes de chiffrement.
- Expliquer les différents types d'attaques sur les systèmes de chiffrement.
- Se familiariser avec les codes correcteurs d'erreurs et leurs applications.
- Comprendre les techniques d'attaques physiques, en particulier celles ciblant les cartes à puce, et analyser les stratégies de protection contre ces attaques.

Contenu du cours

Le plan suivant donne un aperçu de l'organisation temporelle des activités d'apprentissage liées aux séances magistrales. Bien que nous respecterons en gros cette structure générale, les contenus particuliers peuvent changer pour répondre aux besoins.

- **Cours 1**
  Introduction, présentation du cours, du syllabus.
  Présentation du professeur et de ses recherches.
  Discussion sur le cours. Cryptographie classique vs moderne. Types d'attaques. Principe de Kerckhoff. Cryptographie symétrique vs asymétrique. Longueur de clé. Objectifs de la cryptographie. Codes correcteurs d'erreurs.

- **Cours 2**
  Étude des crypto systèmes classiques : chiffrement par décalage, chiffrement par fonction affine, chiffrement de Vigenère, chiffrement de Hill, One-time pads, Enigma et de leurs vulnérabilités. Chiffrements par bloc : ECB, CBC, CFB. Propriétés de Shannon. Génération de bits pseudo-aléatoires.

- **Cours 3-4**
  Le Data Encryption Standard (DES) : historique, algorithme de chiffrement, cryptanalyse différentielle, modes d'opération, les vulnérabilités du DES, les différentes attaques possibles.

- **Cours 5**
  Le Advanced Encryption Standard (AES) : historique, algorithme de chiffrement, le corps fini $GF(2^8)$, construction de la S-box, algorithme de déchiffrement, S-box inverse, les considérations conceptuelles.

- **Cours 6-7**
  Le RSA : historique, rappel de quelques notions mathématiques, l'algorithme RSA, applications, les attaques possibles, tests de primalité, algorithmes de factorisation, concept de clé publique.

- **Cours 8-9**
  Les logarithmes discrets : introduction, calculer des logarithmes discrets, algorithme de Pohlig-Hellman, principe pas de bébé pas de géant, le calcul de l'indice, l'échange de clé Diffie-Hellman, le crypto système ElGamal.

- **Cours 10**
  Les signatures digitales : les signatures RSA, la signature ElGamal, l'algorithme DSA, vulnérabilités.

- **Cours 11**
  Les courbes elliptiques : les courbes elliptiques modulo p, logarithmes discrets sur les courbes elliptiques, factorisation à l'aide des courbes elliptiques, cryptosystème à courbe elliptique.

- **Cours 12**
  Les fonctions de hachage et l'argent digital : le Secure Hash Algorithm (SHA-1), exempled'argent digital élémentaire.

  Techniques d'attaques physique sur les cartes a puce et les possible mesures de sécurités.

- **Cours 13-14**
  Présentations orales.

- **Cours 15**
  Examen final.

Évaluation

L'évaluation consistera en les éléments suivants :

- Un travail s'échelonnant sur l'ensemble de la session, portant sur un sujet au choix de l'étudiant relatif au contenu de cours. Le travail consiste en un compte-rendu de la lecture d'articles scientifiques autour du thème choisi. Le travail s'effectue en équipe de deux. Tout retard entraînera la note **0** à moins d'une entente prise avec le professeur. L'évaluation du travail sera composée des éléments suivants :
    - Une proposition de projet de 2 à 3 pages, à avant remettre le **31 mai 2024** et qui comptera pour **5 points**
    - Une présentation lors des séances du 17 **juin 2024 et du 21 juin 2024** qui consistera en un exposé. Les évaluations du professeur et du groupe compteront à parts égales pour un total de **15 points**
    - Un rapport final à remettre lors du dernier cours, soit le **23 juin 2024** pour une valeur de **30 pts**.
- Un résumé de deux articles scientifiques qui seront fournis par le professeur. Ce travail sera à remettre, au plus tard, le mardi **8 juin 2024**. Ce travail pratique comptera pour **20 points**.
- Un examen final à la séance du **25 juin 2024**. Cet examen est d'une durée de 3 heures et comptera pour **30 points**.

La note finale, sur 100, est la somme de toutes ces évaluations. La note de passage est fixée à 60% ou C.

Formule pédagogique

Le cours sera dispensé en classe par un professeur. Il n'y aura pas de séances de travaux pratiques associées à ce cours.

Situation du cours dans le programme

Le cours est optionnel pour les étudiants inscrits aux programmes de cycles supérieurs. Aucun cours ne lui est préalable.

Références

Aucun manuel ou notes de cours n'est obligatoire pour ce cours. Les diapositives utilisées pendant les cours magistraux seront disponibles via Moodle.

Les références suivantes sont suggérées.

- J. Buchmann. (2006). Introduction à la cryptographie, Dunod Édition, ISBN : 2-10-049622-0.
- Jonathan Katz, Yehuda Lindell (2020). Introduction to Modern Cryptography. Chapman and Hall/CRCTaylor and Francis Group.
- Menezes, P. Van Oorschot and S. Vanstone. Handbook of applied cryptography. CRC Press publisher, *https://cacr.uwaterloo.ca/hac/*.
- D. R. Stinson., Maura B. Paterson (2018). Cryptography : Theory and practice. Chapman and Hall/CRC Taylorand Francis Group, ISBN : 9781138197015.
- Damien Vergnaud. (2012). Exercices et problèmes de cryptographie, Dunod Édition, ISBN :978-2-10-057340-0.
- Bruce Schneier. (2001). Cryptographie appliquée. Protocoles, algorithmes et codes cource en C. ISBN : 9782711786763.
- Paar, Christof, and Jan Pelzl. Understanding cryptography: a textbook for students and practitioners. Springer Science & Business Media, 2009.