Ecole Supérieure Polytechnique
Laboratoire d'Informatique,
de Télécommunications et Applications
LITA

Crytopgraphie et Cryptanalyse

Pr Gervais MENDY
gervais.mendy@esp.sn

Département Génie Informatique, École Supérieure Polytechnique ESP-UCAD

March 13, 2024

Plan

Plan du chapitre 1

Présentation générale de la cryptographie

- Histoire et Évolution de la cryptographie

Plan du chapitre 1

Présentation générale de la cryptographie

- Histoire et Évolution de la cryptographie
- Cryptographie Moderne
  - Caractéristique de la cryptographie moderne
  - Les services de sécurité de la cryptographie
  - Les primitives cryptographiques

Plan du chapitre 1

Présentation générale de la cryptographie

- Histoire et Évolution de la cryptographie
- Cryptographie Moderne
  - Caractéristique de la cryptographie moderne
  - Les services de sécurité de la cryptographie
  - Les primitives cryptographiques
- Cryptosystèmes
  - Les composantes d'un cryptosystème
  - Les types de cryptosystème
  - Principe de Kerckhoff

Plan du chapitre 1

Présentation générale de la cryptographie

- Histoire et Évolution de la cryptographie
- Cryptographie Moderne
  - Caractéristique de la cryptographie moderne
  - Les services de sécurité de la cryptographie
  - Les primitives cryptographiques
- Cryptosystèmes
  - Les composantes d'un cryptosystème
  - Les types de cryptosystème
  - Principe de Kerckhoff
- Introduction à la cryptanalyse: attaques sur les cryptosystèmes
  - Attaques passives; Attaques actives
  - Attaques cryptographiques; Caractère pratique des attaques

Plan du chapitre 2

Éléments mathématiques

- Les éléments algébriques
  - Groupes
  - Anneaux

Plan du chapitre 2

Éléments mathématiques

- Les éléments algébriques
  - Groupes
  - Anneaux
- Les éléments de la théorie des nombres
  - Propriétés de divisibilité
  - Arithmétique modulaire
  - Quelques algorithmes de base de la théorie des nombres

Plan du chapitre 3

Les chiffrements

- Chiffrement par substitution
  - Substitution mono-alphabétique
  - Substitution poly-alphabétique

Plan du chapitre 3

Les chiffrements

- Chiffrement par substitution
  - Substitution mono-alphabétique
  - Substitution poly-alphabétique
- Chiffrement par transposition

Plan du chapitre 4

Chapitre 4

- Chiffrements par blocs

Plan du chapitre 4

Chapitre 4

- Chiffrements par blocs
- Définitions et modes opératoires

Plan du chapitre 4

Chapitre 4

- Chiffrements par blocs
- Définitions et modes opératoires
- Le Data Encryption Standard (DES)

Plan du chapitre 5

Chapitre 5

- RSA

Plan du chapitre 5

Chapitre 5

- RSA
- Rabin

Plan du chapitre 5

Chapitre 5

- RSA
- Rabin
- ElGamal

Plan du chapitre 6

Chapitre 5

- Notions de fonction de hachage cryptographique

Plan du chapitre 6

Chapitre 5

- Notions de fonction de hachage cryptographique
- Classification et propriétés des fonctions de hachage

Plan du chapitre 6

Chapitre 5

- Notions de fonction de hachage cryptographique
- Classification et propriétés des fonctions de hachage
- Conception des fonctions de hachage

Bibliographie et Objectifs du cours

Références

- Introduction à l'algorithmique (Thomas Cormen, Charles Leiserson, Ronald Rivest, Clifford Stein)

Bibliographie et Objectifs du cours

Références

- Introduction à l'algorithmique (Thomas Cormen, Charles Leiserson, Ronald Rivest, Clifford Stein)
- Handbook of applied Cryptography, Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone

Bibliographie et Objectifs du cours

Références

- Introduction à l'algorithmique (Thomas Cormen, Charles Leiserson, Ronald Rivest, Clifford Stein)
- Handbook of applied Cryptography, Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone
- Cryptography: An Introduction (3rd Edition) Nigel Smart

Bibliographie et Objectifs du cours

Références

- Introduction à l'algorithmique (Thomas Cormen, Charles Leiserson, Ronald Rivest, Clifford Stein)
- Handbook of applied Cryptography, Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone
- Cryptography: An Introduction (3rd Edition) Nigel Smart
- Cryptography Engineering: Design Principles and Practical Applications, Niels Ferguson Bruce Schneier Tadayoshi Kohno

Bibliographie et Objectifs du cours

Références

- Introduction à l'algorithmique (Thomas Cormen, Charles Leiserson, Ronald Rivest, Clifford Stein)
- Handbook of applied Cryptography, Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone
- Cryptography: An Introduction (3rd Edition) Nigel Smart
- Cryptography Engineering: Design Principles and Practical Applications, Niels Ferguson Bruce Schneier Tadayoshi Kohno
- Cours de mathématiques: tome 1 Structures fondamentales; tome 2 Polynômes et Algèbre linéaire (Alfred Doneddu)

Bibliographie et Objectifs du cours

Références

- Introduction à l'algorithmique (Thomas Cormen, Charles Leiserson, Ronald Rivest, Clifford Stein)
- Handbook of applied Cryptography, Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone
- Cryptography: An Introduction (3rd Edition) Nigel Smart
- Cryptography Engineering: Design Principles and Practical Applications, Niels Ferguson Bruce Schneier Tadayoshi Kohno
- Cours de mathématiques: tome 1 Structures fondamentales; tome 2 Polynômes et Algèbre linéaire (Alfred Doneddu)
- Cryptographie Appliquée de Bruce Schneier

Bibliographie et Objectifs du cours

Références

- Introduction à l'algorithmique (Thomas Cormen, Charles Leiserson, Ronald Rivest, Clifford Stein)
- Handbook of applied Cryptography, Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone
- Cryptography: An Introduction (3rd Edition) Nigel Smart
- Cryptography Engineering: Design Principles and Practical Applications, Niels Ferguson Bruce Schneier Tadayoshi Kohno
- Cours de mathématiques: tome 1 Structures fondamentales; tome 2 Polynômes et Algèbre linéaire (Alfred Doneddu)
- Cryptographie Appliquée de Bruce Schneier
- SageMath Book, etc.

Prérequis

Prérequis

- Mathématiques: algèbre, arithmétique, théorie des nombres, Probabilité

Prérequis

Prérequis

- Mathématiques: algèbre, arithmétique, théorie des nombres, Probabilité
- Algorithmique: notions de complexité

Objectifs

Objectifs

- OG 1: Connaître les concepts fondamentaux de la cryptographie

Objectifs

Objectifs

- OG 1: Connaître les concepts fondamentaux de la cryptographie
- Analyser et comprendre les Chiffrements historiques

Objectifs

Objectifs

- OG 1: Connaître les concepts fondamentaux de la cryptographie
- Analyser et comprendre les Chiffrements historiques
- Maîtriser les outils mathématiques de la cryptographie
  - Comprendre l'Arithmétique modulaire
  - Se familiariser avec les groupes et les champs finis
  - Apprendre des techniques de base comme les algorithmes d'Euclide, le théorème du reste chinois, etc.

Objectifs

Objectifs

- OG 1: Connaître les concepts fondamentaux de la cryptographie
- Analyser et comprendre les Chiffrements historiques
- Maîtriser les outils mathématiques de la cryptographie
  - Comprendre l'Arithmétique modulaire
  - Se familiariser avec les groupes et les champs finis
  - Apprendre des techniques de base comme les algorithmes d'Euclide, le théorème du reste chinois, etc.
- Comprendre les principes de la cryptographie à clef secrète

Objectifs

Objectifs

- OG 1: Connaître les concepts fondamentaux de la cryptographie
- Analyser et comprendre les Chiffrements historiques
- Maîtriser les outils mathématiques de la cryptographie
  - Comprendre l'Arithmétique modulaire
  - Se familiariser avec les groupes et les champs finis
  - Apprendre des techniques de base comme les algorithmes d'Euclide, le théorème du reste chinois, etc.
- Comprendre les principes de la cryptographie à clef secrète
- Comprendre les principes de la cryptographie à clef publique

Objectifs

Objectifs

- OG 1: Connaître les concepts fondamentaux de la cryptographie
- Analyser et comprendre les Chiffrements historiques
- Maîtriser les outils mathématiques de la cryptographie
  - Comprendre l'Arithmétique modulaire
  - Se familiariser avec les groupes et les champs finis
  - Apprendre des techniques de base comme les algorithmes d'Euclide, le théorème du reste chinois, etc.
- Comprendre les principes de la cryptographie à clef secrète
- Comprendre les principes de la cryptographie à clef publique
- OG2: Mettre en oeuvre des scénarios sur les échecs cryptographiques

Volume Horaire

CM et Exposés

- Cours: 08h

Volume Horaire

CM et Exposés

- Cours: 08h
- TD, TP, Présentation des Travaux: 16h

Évaluations et déroulement des séances

Evaluation

- Animation et participaton individuelle: 25%

Évaluations et déroulement des séances

Evaluation

- Animation et participaton individuelle: 25%
- Evaluation individuelle en classe: 50%

Évaluations et déroulement des séances

Evaluation

- Animation et participaton individuelle: 25%
- Evaluation individuelle en classe: 50%
- Rapport (par groupe) à rendre 05 jours après le séminaire.

Fin de la Présentation

Merci de votre Attention