Arithmétique et Cryptographie : Introduction et Plan

De l'Antiquité au XIX^{e} siècle

- Motivations militaires et diplomatiques
- Vise uniquement la **confidentialité** des communications
- Le chiffrement repose sur des permutations et des substitutions (mono ou poly) alphabétiques
- Pas de discours théorique, scientifique ou systématique : la cryptographie est un artisanat

De l'Antiquité au XIX^{e} siècle

- Motivations militaires et diplomatiques
- Vise uniquement la **confidentialité** des communications
- Le chiffrement repose sur des permutations et des substitutions (mono ou poly) alphabétiques
- Pas de discours théorique, scientifique ou systématique : la cryptographie est un artisanat

Machine à chiffrer dite d'Henri II (fonctionnement inconnu !)

L'ère de la guerre industrielle

- Importance des communications dans les guerres modernes, les progrès de la cryptographie se font au rythme des conflits majeurs

L'ère de la guerre industrielle

- Importance des communications dans les guerres modernes, les progrès de la cryptographie se font au rythme des conflits majeurs
- Premier texte énonçant des principes systématiques connu sous le nom de *Principes de Kerckhoffs*, en résumé :
  le secret doit résider dans la clef, et non dans le procédé de chiffrement
  (*La cryptographie militaire*, Auguste Kerckhoffs, *Journal des sciences militaires*, 1883)

L'ère de la guerre industrielle

- Importance des communications dans les guerres modernes, les progrès de la cryptographie se font au rythme des conflits majeurs
- Premier texte énonçant des principes systématiques connu sous le nom de *Principes de Kerckhoffs*, en résumé :
  le secret doit résider dans la clef, et non dans le procédé de chiffrement
  (*La cryptographie militaire*, Auguste Kerckhoffs, *Journal des sciences militaires*, 1883)
- Chiffre de Vernam (1917) : *masque jetable*, ou *one-time pad*
  (en fait un *Chiffre de Vigenère*, avec clef aléatoire à usage unique)

L'ère de la guerre industrielle

- Importance des communications dans les guerres modernes, les progrès de la cryptographie se font au rythme des conflits majeurs
- Premier texte énonçant des principes systématiques connu sous le nom de *Principes de Kerckhoffs*, en résumé :
  le secret doit résider dans la clef, et non dans le procédé de chiffrement
  (*La cryptographie militaire*, Auguste Kerckhoffs, *Journal des sciences militaires*, 1883)
- Chiffre de Vernam (1917) : *masque jetable*, ou *one-time pad*
  (en fait un *Chiffre de Vigenère*, avec clef aléatoire à usage unique)
- Cassage du code *Enigma* à l'aide de la *Bombe* (électromécanique), par l'équipe d'Alan Turing, à Bletchley Park (1942)

L'ère de la guerre industrielle

- Importance des communications dans les guerres modernes, les progrès de la cryptographie se font au rythme des conflits majeurs
- Premier texte énonçant des principes systématiques connu sous le nom de *Principes de Kerckhoffs*, en résumé :
  le secret doit résider dans la clef, et non dans le procédé de chiffrement
  (*La cryptographie militaire*, Auguste Kerckhoffs, *Journal des sciences militaires*, 1883)
- Chiffre de Vernam (1917) : *masque jetable*, ou *one-time pad*
  (en fait un *Chiffre de Vigenère*, avec clef aléatoire à usage unique)
- Cassage du code *Enigma* à l'aide de la *Bombe* (électromécanique), par l'équipe d'Alan Turing, à Bletchley Park (1942)
- *Colossus*, 1944 : première machine électronique utilisée pour briser les codes allemands

L'ère de la guerre industrielle

- Importance des communications dans les guerres modernes, les progrès de la cryptographie se font au rythme des conflits majeurs
- Premier texte énonçant des principes systématiques connu sous le nom de *Principes de Kerckhoffs*, en résumé :
  le secret doit résider dans la clef, et non dans le procédé de chiffrement
  (*La cryptographie militaire*, Auguste Kerckhoffs, *Journal des sciences militaires*, 1883)
- Chiffre de Vernam (1917) : *masque jetable*, ou *one-time pad*
  (en fait un *Chiffre de Vigenère*, avec clef aléatoire à usage unique)
- Cassage du code *Enigma* à l'aide de la *Bombe* (électromécanique), par l'équipe d'Alan Turing, à Bletchley Park (1942)
- *Colossus*, 1944 : première machine électronique utilisée pour briser les codes allemands
- Claude Shannon (*Théorie de l'information*, 1948) : formalisation (probabilités) de concepts cryptographiques (sûreté parfaite, ou *sémantique*), *confusion*, *diffusion*

Les Années 70 : Double révolution

Explosion des besoins en cryptographie : systèmes informatiques, communications, y compris dans le domaine civil.

Les Années 70 : Double révolution

Explosion des besoins en cryptographie : systèmes informatiques, communications, y compris dans le domaine civil.

- Invention de la cryptographie à clef publique, comme idée, puis comme technologie
- Premier Standard de chiffrement par blocs, plus ou moins universel : DES

RSA,
de droite à gauche
(Source : usc.edu)

Cryptographie à clef publique

- Début des années 70 : Idée de fonction à sens unique avec porte dérobée (*trapdoor one-way function*)

Cryptographie à clef publique

- Début des années 70 : Idée de fonction à sens unique avec porte dérobée (*trapdoor one-way function*)
- 1976 : *New Directions in Cryptography*
  Article fondateur de Diffie et Hellman proposant un mécanisme d'échange secret d'informations sans partage préalable d'une clef secrète

Cryptographie à clef publique

- Début des années 70 : Idée de fonction à sens unique avec porte dérobée (*trapdoor one-way function*)
- 1976 : *New Directions in Cryptography*
  Article fondateur de Diffie et Hellman proposant un mécanisme d'échange secret d'informations sans partage préalable d'une clef secrète
- 1977 : *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems*
  Article présentant RSA (Rivest, Shamir, et Adleman), premier exemple concret d'algorithme de chiffrement à clef publique

Cryptographie à clef publique

- Début des années 70 : Idée de fonction à sens unique avec porte dérobée (*trapdoor one-way function*)
- 1976 : *New Directions in Cryptography*
  Article fondateur de Diffie et Hellman proposant un mécanisme d'échange secret d'informations sans partage préalable d'une clef secrète
- 1977 : *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems*
  Article présentant RSA (Rivest, Shamir, et Adleman), premier exemple concret d'algorithme de chiffrement à clef publique
- Puis procédés d'Elgamal, de Rabin, courbes elliptiques ...
  Tous ces algorithmes reposent sur la difficulté supposée de problèmes classiques en théorie des nombres

Standards de chiffrement par blocs

- 1977 : publication du standard DES (*Data Encryption Standard*, FIPS PUB 46), issu du programme Lucifer d'IBM
- L'algorithme met en œuvre les concepts dégagés par Shannon : confusion et diffusion
- Jamais « cassé », mais la clé trop courte (56 bits) rend le chiffrement vulnérable à une attaque par force brute dès la fin des années 90.
  DES est abandonné en 2000, sauf dans le *triple DES*.

Standards de chiffrement par blocs

- 1977 : publication du standard DES (*Data Encryption Standard*, FIPS PUB 46), issu du programme Lucifer d'IBM
- L'algorithme met en œuvre les concepts dégagés par Shannon : confusion et diffusion
- Jamais « cassé », mais la clé trop courte (56 bits) rend le chiffrement vulnérable à une attaque par force brute dès la fin des années 90.
  DES est abandonné en 2000, sauf dans le *triple DES*.
- 2000 : adoption par le NIST du standard AES (*Advanced Encryption Standard*, FIPS PUB 197), adapté de l'algorithme Rijndael (J. Daemen et V. Rijmen, 1998), à l'issue dun concours international
- Les clés AES sont de 128 bits, voire 192 ou 256 bits.
  Une attaque par force brute semble *physiquement* impossible.

Aujourd'hui ?

- Tout le monde utilise la cryptographie, tout le temps :
  échanges de données, authentification, transactions bancaires ...

Aujourd'hui ?

- Tout le monde utilise la cryptographie, tout le temps :
  échanges de données, authentification, transactions bancaires ...
- Les outils cryptographiques doivent assurer :
  1. La confidentialité (chiffrement proprement dit)
  2. L'intégrité des échanges
  3. L'authentification (y compris signature)

Aujourd'hui ?

- Tout le monde utilise la cryptographie, tout le temps :
  échanges de données, authentification, transactions bancaires ...
- Les outils cryptographiques doivent assurer :
  1. La confidentialité (chiffrement proprement dit)
  2. L'intégrité des échanges
  3. L'authentification (y compris signature)
- Les protocoles/logiciels en usage mêlent
  - cryptographie à clé publique (lente) : échange des clés, signatures
  - et à clé privée, ou symétrique (environ 1000 fois plus rapide) :
    chiffrement des données

$\rightarrow$ ssh, ssl, pgp, ...

Plan du cours

1. Arithmétique des entiers
   (divisibilité, algorithme d'Euclide, factorisation)
2. Arithmétique modulaire
   (classes de congruence, structure d'anneau, groupe des unités),
   applications à la cryptographie à clef publique
3. Arithmétique des polynômes
   (anneaux de polynômes, division euclidienne, anneaux quotients),
   applications au CRC, et à Rijndael/AES