L'épreuve de modélisation

Le 29 septembre 2017

Le texte

`https://agreg.org/Textes/public2018-C2.pdf`

Un texte publié cette année portant sur le schéma de chiffrement RSA et sur différentes attaques (clés faibles) de ce dernier.

Remarques sur le texte

- Thème : arithmétique effective, $\mathbf{Z}/n\mathbf{Z}$;
- Les parties du texte sont relativement indépendantes (ce n'est pas le cas de tous les textes).
- Niveau progressif :
  - §1. Présentation du système RSA (classique) ;
  - §2. Application du théorème Chinois ;
  - §3. Structure de $(\mathbf{Z}/n\mathbf{Z})^\times$, indicatrice d'Euler ;
  - §4. Carrés dans $\mathbf{Z}/n\mathbf{Z}$, factorisation ;
  - §5. Approximation diophantienne, fractions continues.

Remarques sur le texte

- Thème : arithmétique effective, $\mathbf{Z}/n\mathbf{Z}$;
- Les parties du texte sont relativement indépendantes (ce n'est pas le cas de tous les textes).
- Niveau progressif :
  - §1. Présentation du système RSA (classique) ;
  - §2. Application du théorème Chinois ;
  - §3. Structure de $(\mathbf{Z}/n\mathbf{Z})^\times$, indicatrice d'Euler ;
  - §4. Carrés dans $\mathbf{Z}/n\mathbf{Z}$, factorisation ;
  - §5. Approximation diophantienne, fractions continues. (De jolies choses pour la nouvelle leçon **142**)

Proposition de plan

(1) Le système RSA.
(2) Clés faibles de RSA :
    (a) Clés publiques faibles ;
    (b) Clés secrètes faibles.
(3) Synthèse : proposition de paramètres fiables.

Introduction

- Dégager la problématique soulevée par le texte : cryptographie. Motiver l'utilisation du chiffrement sur un exemple concret : internet, cartes bleues etc...
- But du texte : présenter des attaques pour certains choix de clés/paramètres. À quoi ces attaques peuvent servir ?

Introduction

- Dégager la problématique soulevée par le texte : cryptographie. Motiver l'utilisation du chiffrement sur un exemple concret : internet, cartes bleues etc...
- But du texte : présenter des attaques pour certains choix de clés/paramètres. À quoi ces attaques peuvent servir ?
  $\rightarrow$ Aider l'utilisateur dans ses choix de paramètres.

Introduction

- Dégager la problématique soulevée par le texte : cryptographie. Motiver l'utilisation du chiffrement sur un exemple concret : internet, cartes bleues etc...
- But du texte : présenter des attaques pour certains choix de clés/paramètres. À quoi ces attaques peuvent servir ?
  $\rightarrow$ Aider l'utilisateur dans ses choix de paramètres.

Remarque

Aucune notion de cryptographie n'est explicitement au programme de l'option sauf (nouveau programme 2018) une mention à RSA.

Le système RSA

- Présentation succincte ; expliquer pourquoi le système fonctionne ; attention au cas où p ou q divise m.
- Avantage de l'utilisateur sur un attaquant ; pourquoi l'attaquant ne peut-il pas raisonnablement tester toutes les clés secrètes ?
  - $\rightarrow$ Exponentiation rapide. Discuter la complexité du chiffrement/déchiffrement.

Clés publiques faibles

Cas d'un petit exposant public e. Motivation : chiffrement rapide.

- Cas d'une diffusion massive d'un message avec un exposant commun. Coalition d'utilisateurs.

- Calcul d'une racine n-ième dans $\mathbf{Z}$.

Clés publiques faibles

Cas d'un petit exposant public e. Motivation : chiffrement rapide.

- Cas d'une diffusion massive d'un message avec un exposant commun. Coalition d'utilisateurs.
  - $\rightarrow$ Théorème Chinois.

- Calcul d'une racine n-ième dans $\mathbf{Z}$.

Clés publiques faibles

Cas d'un petit exposant public e. Motivation : chiffrement rapide.

- Cas d'une diffusion massive d'un message avec un exposant commun. Coalition d'utilisateurs.
  - $\rightarrow$ Théorème Chinois.
  - $\rightarrow$ On peut discuter la réalisation effective : algorithme d'Euclide étendu.

- Calcul d'une racine n-ième dans $\mathbf{Z}$.

Clés publiques faibles

Cas d'un petit exposant public e. Motivation : chiffrement rapide.

- Cas d'une diffusion massive d'un message avec un exposant commun. Coalition d'utilisateurs.
  - $\rightarrow$ Théorème Chinois.
  - $\rightarrow$ On peut discuter la réalisation effective : algorithme d'Euclide étendu.
  - $\rightarrow$ Discuter la complexité (piste noire).
- Calcul d'une racine n-ième dans $\mathbf{Z}$.

Clés publiques faibles

Cas d'un petit exposant public e. Motivation : chiffrement rapide.

- Cas d'une diffusion massive d'un message avec un exposant commun. Coalition d'utilisateurs.
  - $\rightarrow$ Théorème Chinois.
  - $\rightarrow$ On peut discuter la réalisation effective : algorithme d'Euclide étendu.
  - $\rightarrow$ Discuter la complexité (piste noire).
- Calcul d'une racine n-ième dans $\mathbf{Z}$.
  - $\rightarrow$ méthodes de dichotomie, méthode de Newton.

Clés publiques faibles

Cas d'un petit exposant public e. Motivation : chiffrement rapide.

- Cas d'une diffusion massive d'un message avec un exposant commun. Coalition d'utilisateurs.
  - $\rightarrow$ Théorème Chinois.
  - $\rightarrow$ On peut discuter la réalisation effective : algorithme d'Euclide étendu.
  - $\rightarrow$ Discuter la complexité (piste noire).
- Calcul d'une racine n-ième dans $\mathbf{Z}$.
  - $\rightarrow$ méthodes de dichotomie, méthode de Newton.
  - $\rightarrow$ Étude de complexité, s'adapter au contexte : on recherche une solution entière !

Clés publiques faibles II

- Exposant public e d'ordre petit dans $(\mathbf{Z}/\varphi(n)\mathbf{Z})^\times$: il suffit d'itérer le chiffrement pour déchiffrer. Une proposition donne un majorant de la probabilité que d soit petit pour une clé publique e aléatoire.

Clés publiques faibles II

- Exposant public e d'ordre petit dans $(\mathbf{Z}/\varphi(n)\mathbf{Z})^\times$: il suffit d'itérer le chiffrement pour déchiffrer. Une proposition donne un majorant de la probabilité que d soit petit pour une clé publique e aléatoire.
  - $\rightarrow$ Illustration informatique. Comparer cette majoration avec des résultats expérimentaux.

Clés publiques faibles II

- Exposant public e d'ordre petit dans $(\mathbf{Z}/\varphi(n)\mathbf{Z})^\times$: il suffit d'itérer le chiffrement pour déchiffrer. Une proposition donne un majorant de la probabilité que d soit petit pour une clé publique e aléatoire.
  - $\rightarrow$ Illustration informatique. Comparer cette majoration avec des résultats expérimentaux.

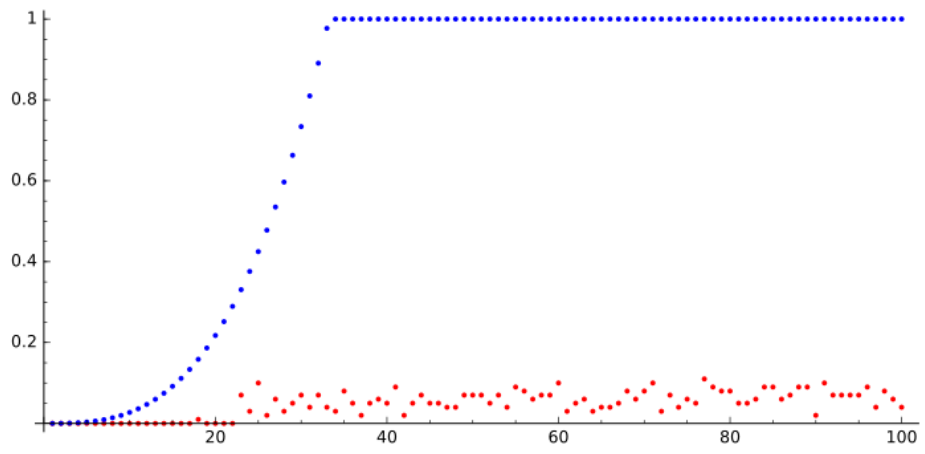

Figure – Estimations de la probabilité que d soit d'ordre inférieur à δ (en abscisse). Borne théorique en bleu, espérances empiriques en rouge.

Clés secrètes faibles

Piste noire. Partie moins guidée, plus technique, plus de mathématiques à détailler.

Synthèse, paramètres fiables

- Proposer une clé publique e telle que e assez grand. $e \gg$ nombre de destinataires dans le cas d'une diffusion massive
- Attention à e d'ordre petit dans $(\mathbf{Z}/\varphi(n)\mathbf{Z})^\times$;
- e tel que $d \gg \frac{1}{3}\sqrt[4]{n}$. Pour un e aléatoire, $\mathbf{P}(d > \frac{1}{3}\sqrt[4]{n}) \geq \frac{3\varphi(n)}{\sqrt[4]{n}}$
  $\rightarrow$ Valeurs numériques sur des exemples bien choisis.

Synthèse, paramètres fiables

- Proposer une clé publique e telle que e assez grand. $e \gg$ nombre de destinataires dans le cas d'une diffusion massive
- Attention à e d'ordre petit dans $(\mathbf{Z}/\varphi(n)\mathbf{Z})^\times$;
- e tel que $d \gg \frac{1}{3}\sqrt[4]{n}$. Pour un e aléatoire, $\mathbf{P}(d > \frac{1}{3}\sqrt[4]{n}) \geq \frac{3\varphi(n)}{\sqrt[4]{n}}$
  $\rightarrow$ Valeurs numériques sur des exemples bien choisis.
- n assez grand pour que la factorisation soit difficile ; p et q du même ordre de grandeur... mais pas trop proches quand même.

Illustrations informatiques possibles

- Illustrer un chiffrement et déchiffrement RSA sur un exemple jouet puis sur des exemples plus conséquents. $\rightarrow$ Montrer des temps de calcul en fonction de l'exposant et de n. Prendre un exposant "générique" puis un exposant de la forme $2^s + 1$ (comme suggéré en fin de §2).

Illustrations informatiques possibles

- Illustrer un chiffrement et déchiffrement RSA sur un exemple jouet puis sur des exemples plus conséquents. $\rightarrow$ Montrer des temps de calcul en fonction de l'exposant et de n. Prendre un exposant "générique" puis un exposant de la forme $2^s + 1$ (comme suggéré en fin de §2).
- Tester un algorithme de factorisation naïf (recherche exhaustive de facteurs jusqu'à $\sqrt{n}$) et afficher les temps de calcul. Tester un algorithme de recherche exhaustive de clé secrète. Comparer avec les temps de chiffrement/déchiffrement.

Illustrations informatiques possibles

- Illustrer un chiffrement et déchiffrement RSA sur un exemple jouet puis sur des exemples plus conséquents. $\rightarrow$ Montrer des temps de calcul en fonction de l'exposant et de n. Prendre un exposant "générique" puis un exposant de la forme $2^s + 1$ (comme suggéré en fin de §2).
- Tester un algorithme de factorisation naïf (recherche exhaustive de facteurs jusqu'à $\sqrt{n}$) et afficher les temps de calcul. Tester un algorithme de recherche exhaustive de clé secrète. Comparer avec les temps de chiffrement/déchiffrement.
- §3 : Comparer la majoration sur la probabilité que e soit d'ordre petit avec des moyennes empiriques sur des exemples. $\rightarrow$ Comparaison graphique.

Illustrations informatiques possibles

- Illustrer un chiffrement et déchiffrement RSA sur un exemple jouet puis sur des exemples plus conséquents. $\rightarrow$ Montrer des temps de calcul en fonction de l'exposant et de n. Prendre un exposant "générique" puis un exposant de la forme $2^s + 1$ (comme suggéré en fin de §2).
- Tester un algorithme de factorisation naïf (recherche exhaustive de facteurs jusqu'à $\sqrt{n}$) et afficher les temps de calcul. Tester un algorithme de recherche exhaustive de clé secrète. Comparer avec les temps de chiffrement/déchiffrement.
- §3 : Comparer la majoration sur la probabilité que e soit d'ordre petit avec des moyennes empiriques sur des exemples. $\rightarrow$ Comparaison graphique.
- §4 (non traité dans ce qui précède) : illustrer les résultats probabilistes présentés sur des exemples.

Illustrations informatiques possibles

- Illustrer un chiffrement et déchiffrement RSA sur un exemple jouet puis sur des exemples plus conséquents. $\rightarrow$ Montrer des temps de calcul en fonction de l'exposant et de n. Prendre un exposant "générique" puis un exposant de la forme $2^s + 1$ (comme suggéré en fin de §2).
- Tester un algorithme de factorisation naïf (recherche exhaustive de facteurs jusqu'à $\sqrt{n}$) et afficher les temps de calcul. Tester un algorithme de recherche exhaustive de clé secrète. Comparer avec les temps de chiffrement/déchiffrement.
- §3 : Comparer la majoration sur la probabilité que e soit d'ordre petit avec des moyennes empiriques sur des exemples. $\rightarrow$ Comparaison graphique.
- §4 (non traité dans ce qui précède) : illustrer les résultats probabilistes présentés sur des exemples.
- §4 Implémenter l'algorithme de factorisation décrit dans cette section (plus risqué).

Des questions ?