TD2 - chiffrements asymétriques

September 2022

1 Introduction

Objectif: manipuler les différents concepts d'arithmétique modulaire appliqués au chiffrement RSA et commencer à réfléchir sur l'implémentation de ce chiffrement pour préparer le TP.
Prérequis:

- connaître le fonctionnement de RSA
- se rappeler de l'algorithme d'Euclide

Connaissances à acquérir:

- utiliser l'algorithme d'Euclide et l'algorithme d'Euclide étendu
- calculer l'inverse d'un nombre sur un ensemble Z/nZ
- calculer une exponentiation modulaire
- chiffrer et déchiffrer un message avec RSA

Instructions: Réaliser ces exercices en groupes de 3 (maximum).

2 Echauffement

2.1 Bachet-Bézout

Le maire de Gotham City souhaite changer de monnaie et réimprimer tous les billets de la ville pour simplifier les transactions. Il souhaiterait savoir s'il est judicieux (ou non) de n'utiliser des billets que de deux valeurs différentes. Il aimerait notamment savoir si les habitants seraient toujours capable d'acheter tout types de produits. Pour chaque proposition du maire, expliquez si oui ou non, les valeurs des billets permettent aux habitants d'acheter des produits de n'importe quelles valeurs:

- 7 et 19
- 29 et 38
- 111 et 53

2.2 Calcul d'inverses

Le maire de Gotham vous remercie pour vos conseils. Il souhaite maintenant que vous calculiez les inverses de nombres sur des ensembles Z/nZ. Sans raison particulière, il trouve ça rigolo.

- calculez l'inverse de 5 sur Z/26Z.
- calculez l'inverse de 17 sur Z/46Z.
- calculez l'inverse de 47 sur Z/51Z.

2.3 Exponentiations modulaires

L'adjoint au maire aime également beaucoup l'arithmétique modulaire, il vous demande de calculer (de tête) les exponentiations modulaires suivantes:

- $x \equiv 10^5 \pmod{85}$
- $x \equiv 4^8 \pmod{26}$
- $x \equiv 12^5 \pmod{122}$

3 Chiffrement RSA

Batman et Robin souhaitent communiquer discrètement pour que leurs messages ne soient ni lus ni modifiés par le Joker. Pour cela, ils décident d'utiliser le bat-ordinateur pour développer un bat-programme utilisant RSA pour chiffrer et déchiffrer des messages. Malheureusement, Batman et Robin n'ont pas eu le temps de se former à la cryptographie. Ils vous demande de leur donner un exemple du fonctionnement de RSA en chiffrant et déchiffrant le message suivant: *LES CAROTTES SONT CUITES*.

Pour chiffrer ce message, vous devez d'abord l'encoder sous forme de chiffres en associant chaque lettre à un nombre (A=1, B=2, C=3, *etc.*). Puis chaque nombre doit être chiffré puis déchiffré avec RSA de manière individuelle.

Les paramètres à sélectionner pour chiffrer et déchiffrer le message sont:

- clef publique: $p = 5$, $q = 17$
- exposant: $e = 5$

4 Automatisation

Batman et Robin sont surpris de voir à quel point il est long et fastidieux de chiffrer un message avec RSA. Ils souhaitent que vous leur proposiez un pseudo-code permettant d'automatiser ce processus.

Proposez 3 fonctions en pseudo-code pour les tâches suivantes:

- Génération de clés: la fonction prend en paramètre p, q et e, et retourne n.
- Chiffrement de messages: la fonction prend un caractère déchiffré en paramètre et le retourne chiffré.
- Déchiffrement de messages: la fonction prend un caractère chiffré en paramètre et le retourne déchiffré.

5 Amélioration du Bat-programme

Après moulte réflexions, Batman et Robin ne sont pas bien convaincus par vos propositions. Il en ressort que votre bat-programme semble bien fonctionner mais qu'il est très facile de faire une analyse fréquentielle des caractères pour décrypter les messages.

Cherchez et proposez des mécanismes empêchant une analyse fréquentielle pour rendre votre bat-programme plus sécurisé.