CRY - Laboratoire 2

Exploitation

10 janvier 2021

Étudiants
Doran KAYOUMI

Professeur
Alexandre DUC
Assistant
Olivier KOPP

HAUTE ÉCOLE
D'INGÉNIERIE ET DE GESTION
DU CANTON DE VAUD
www.heig-vd.ch

Table des matières

1 El Gamal

1.1 Chiffrement / Déchiffrement

1.1.1 Génération de la paire de clé

Avant de pouvoir chiffré/déchiffré un message, il nous faut générer une paire de clés publique/privée. Selon la donnée, on génère une valeur secrète $a \in \mathbb{Z}_p$ qui sera la clé privé. Ensuite, la clé publique correspond à $A = ag \ mod \ p$ (**g** étant un générateur de $\mathbb{Z}_p$ qui correspond à l'un des paramètres de cette construction d'El Gamal).

Donc notre paires de clés correspond à (A, a).

1.1.2 Chiffrement

Avant de commencer à faire le calcul mathématique compliqué qui font peur, on va tirer un $b \in \mathbb{Z}_p$ uniformément au hasard. Et donc le texte chiffré correspond à la paire $(u, v) = (bg \ mod \ p, m + bA \ mod \ p)$

1.1.3 Déchiffrement

Le texte clair correspond à $m = v - au \ mod \ p$

1.2 Attaque

Vu que mon "ami" informaticien à décider de travailler dans $\mathbb{Z}_p$ et non dans $\mathbb{Z}_p^*$ (i.e. un groupe additif et non un groupe multiplicatif), le chiffrement et le déchiffrement s'effectue avec de simple addition, soustraction et multiplication et non avec des puissances (ce qui est le cas dans un groupe multiplicatif).

Sachant ça, on peut facilement retrouver la clé privé en faisant une simple division $a = A/g \ mod \ p$ (**A** est la clé publique et **g** l'un des paramètres).

Maintenant que l'on a la clé privée, on peu facilement déchiffrer le message.

Le message : Youuuu Shall Noooot charges

1.3 Sécurité d'El Gamal

La sécurité d'El Gamal à un lien très étroit avec le type de groupe choisi. Avec un groupe additif (ce qui est le cas ici), la clé privée peut être retrouvés facilement en effectuant une simple division. Tandis qu'avec un groupe **multiplicatif**, il faut résoudre le problème du logarithme discret pour retrouver la clé privé ce qui est un problème difficile [1].

1. Néanmoins, il faut utiliser un bon **p** sinon résoudre ce problème devient plus facile

2 Chiffrement avec racines carrées

2.1 Attaque

La première chose que j'ai fait, c'est de trouver un multiple de **p**. Si on essaie de représenter ce multiple dans $\mathbb{Z}_p \times \mathbb{Z}_q$, on obtiens $(0, a)$. Cette valeur peut-être trouvée à l'aide des racines trouvées avec le théorème du reste chinois (a.k.a CRT) $(\pm c_p, \pm c_q)$. Si l'on soustrait la première racine et la troisième, on obtient $(c_p, c_q) - (c_{p,q}) = (0, 2c_q)$. Ce qui correspond à notre $(0, a)$ et donc notre multiple de **p**.

Pour en revenir à l'attaque, nous avons les racines dans $\mathbb{Z}_n$ ce qui ne change en rien la façon de trouver un multiple de **p**. Le problème c'est que l'on ne sait pas à quoi correspond r_1, r_2, r_3 et r_4. Ce qui en soit n'est pas vraiment un problème, il faudra juste tester plusieurs combinaisons différentes. Par exemple, on fixe **roots[0]** et l'on effectue une soustraction avec les trois autres. Sur ces trois calculs, deux nous permettrons de retrouver un multiple de **p** ou de **q** tandis que la troisième pas. Une fois un multiple trouvé, il suffit de calculer le **pgdc** entre ce multiple et **n** et l'on obtiens **p** ou **q**. Ce qui nous permet de retrouver l'autre et donc de déchiffrer le message.

Le message : Ni ! Ni ! Ni ! Ni ! We want a industrially ! You must return here with a industrially or else you will never pass through this wood alive !

3 RSA

3.1 Première solution

Etant donnée que $n = p^4$, j'ai retrouvé **p** en faisant $p = \sqrt[4]{n}$. Une fois **p** retrouvé, j'ai pu recaluler la clé privée et donc retrouver le message.

Le message : What is your quest ? To seek the holy grail. What is your favorite color ? whence

Cette solution n'est pas du tout sûre, car le calcul d'une racine n^e est très facile à faire.

3.2 Deuxième solution

Pour casser cette solution, j'ai simplement calculé $\varphi(n)$ ce qui m'a permis de recalculer la clé privée et donc retrouver le message.

Le message : Always look on the bright side of teargassing

J'ai pu faire ça car **n** est calculé avec beaucoup de nombres premier relativement petit. Ce qui fait que la factorisation de **n** est très facile à faire.

3.3 Troisième solution

J'ai utilisé la première étape de la méthode de factorisation de Fermat [2].

J'ai commencé par trouver le plus petit chiffre, **a**, dont le carré est le plus proche de **n**. Ensuite, j'ai calculé un **b**

- J'ai commencé par trouver le plus petit chiffre dont le carré est le plus proche de **n**. $a = \lceil \sqrt{n} \rceil$
- Puis j'ai trouvé la racine de la différence entre le carré de a et n. $b = \lceil \sqrt{a^2 - n} \rceil$
- $p = a + b$
- $q = a - b$

Une fois **p** et **q** retrouvé, j'ai pu recalculer la clé privée et donc retrouver le message.

Le message : In 2020, we already got the coronavirus and a locust plague. What will we have in 2021 ? misdoings

Etant donnée que **p** et **q** sont relativement proche, cela fais que la racine carré de **n** est proche de p et q. Ce qui réduit considérablement la zone de recherche et facilite la factorisation de **n**.

2. https://en.wikipedia.org/wiki/Fermat%27s_factorization_method#The_basic_method