BSPro - A First Bachelor Semester Project in BiCS-land

Saturday 23rd January, 2021 - 15:45

Issam Jomaa
University of Luxembourg
Email: issam.jomaa.001.student@uni.lu

Răzvan Roşie
University of Luxembourg
Email: razvan.rosie@uni.lu

Abstract

Ce papier présente un résumer d'approximativement 1000 mots, en français du projet de premier semestre fait pas Issam Jomaa sous la tutelle de Răzvan Roşie. Pour plus d'informations le lecteur est invité a lire le rapport en entier écrit en anglais.

1. Introduction

Le but du projet est de crée un programme qui crée et résout des « Time Lock Puzzle » basée sur l'algorithme RSA . Pendant la résolution du « Time Lock Puzzle », le programme devra enregistrée les données en relation avec le temps mis par le programme pour effectuer cette tache. Ce programme sera écrit en langage C++ et Python. Notre but tout au long de ce projet est de se familiariser et d'avoir une connaissance solide en matière de Cryptographie ainsi que les différentes méthodes qui constituent ce domaine. Notre second objectif serait de bien comprendre le fonctionnement du système de chiffrement RSA afin de pouvoir le prendre comme base sur laquelle bâtir notre programme. Etant donnée que ce projet est un projet de première année en Bachelor il est important, si ce n'est crucial d'apprendre et d'améliorée nos compétences en termes de coding concernant le langage Python et C++. A la fin de ce projet en utilisant notre deuxième programme que nous allons crée nous devrions pouvoirs tirée des conclusions non seulement concernant les performances de notre programme mais aussi en général concernant la différence de performance entre Python et C++.

2. Background

Ce projet tourne autour du domaine de la Cryptographie et donc de ce fait autour d'un des 3 principaux types de cryptographie qui est : La cryptographie Asymétrique. C'est une technique qui permet d'envoyer des donnés en toute sécurité cela en la cryptant avec un système de pair de clés qui ont différentes fonctions.

- une clé publique qui est connu de l'envoyeur et du receveur.
- une clé privée ne doit être connu que par le receveur.

L'envoyeur va utiliser sa clé publique connu des deux utilisateur pour crypter les données grâce à un algorithme mathématique. Une fois les données cryptées elle ne peuvent être décryptée que grâce a la clé privée. Cela implique que l'utilisateur qui reçoit n'as besoin que de protéger sa clé privé sans avoir à l'envoyer à travers internet ou à travers quelconques autres méthodes, ce qui veut dire qu'il y'a peu de chance que des personnes peuvent y avoir accès illicitement. Les « Time Lock Puzzle » sont essentiellement basée sur la cryptographie Asymétrique, et celle que nous allons utiliser dans notre projet est basée sur le système RSA. Les « Time Lock Puzzle » sont supposer chiffrer un message de façon a ce que la décryptions de ce message prendra un temps fini que le créateur du puzzle définira avant la création de celui-ci. De ce fait ils ont une grande utilité dans la vie réelle surtout dans certains cas ou des taches sont liées au temps d'où son importance dans des secteurs comme la finance ou bien le chiffrement en général. Finalement nous allons aborder les langage que nous allons utilisé pour écrire nos programmes. Il s'agit d'un langage de programmation interprété de haut niveau et orienté objets. Comparée aux autres langage de programmation Python se distingue par sa lisibilité dues à l'utilisation de mots d'anglais pour la syntaxe comparés aux autres qui utilisent de la ponctuation

et des symboles pour celle-ci. C'est aussi considérer un langage multitâches qui peut être utilisée pour diverses taches.

"C++ est un langage de programmation compilé permettant la programmation sous de multiples paradigmes, dont la programmation procédurale, la programmation orientée objet et la programmation générique. Ses bonnes performances, et sa compatibilité avec le C en font un des langages de programmation les plus utilisés dans les applications où la performance est critique." [1]

3. Exigences, Design et Production

Notre premier exigence globale est d'avoir un programme qui peut être considérer comme professionnel, ce qui veut dire que notre code sera aussi simple et propre que possible ainsi que bien commenter. On évitera tout déchets dans l'écriture de celui-ci. Ceci devrait nous donner un programme écrit avec une qualité qui correspond aux standards de l'industrie. Ensuite une autre exigence concernant notre programme serait d'avoir un programme modulable c'est-à-dire fractionner autant que possible en fonctions afin de faciliter non seulement les modifications mais aussi la maintenance et le débug de celui-ci. Notre programme principal devrait être capable de générer des nombres premier et des clés de chiffrement pour nos time lock puzzle rapidement. Dans le cas du programme écrit en C++ nous allons devoir crée toutes les fonctions nécessaire spécialement celles qui taclent les problèmes de notion d'aléatoire dans notre programme ainsi que la génération des nombres premier. Premièrement nous allons devoir utiliser des grandes variables pour le programme pour cela nous allons utiliser la librairies GNU et plus précisément la classe mpz_class. Nous allons aussi utiliser des fonctions de cette librairie pour l'aléatoire. La génération des nombres premier ce fera avec le test de primalité Miller-Rabin tout en ajoutant quelques conditions pour s'assurer de sa fiabilité. Cette fonctions sera appeler $generateprime()$ et utilisera deux autres fonctions que l'on aura aussi créé $fonctionrandom()$ et $isPrime()$, $isPrime()$ étant le test Miller-Rabin. Une fois la clé crée, la fonctions rsw aura la tache de résoudre le puzzle. Pendant la résolution le programme devra enregistrée le temps pris par celui-ci et l'enregistré dans un fichier avec le bon format que l'on précisera. Le programme en Python aura le même schéma cependant els fonctions liées a l'aléatoire et la génération des nombres premiers seront directement prises d'une librairie. Notre deuxième programme devrait être capable de lire ce fichier de données et de crée un graphique a partir de celui-ci.

4. Conclusion

Apres avoir faire marcher notre programme pendant une longue période de temps et obtenus les fichiers de données du programme principale dans les deux version, nous avons crée les graphiques a l'aide de notre deuxième programme. Nous avons observée a l'aide de ces deux graphiques que le programme en C++ est beaucoup plus rapide que celui en Python et cela avec un grand écarts en ce qui concerne la résolution du puzzle. Nous en avons déduits que cela pourrait être due a la méthode différente entre les deux langages en ce qui concerne le stockage de l'informations dans la mémoire, et que ce stockage dynamique qu'emploie python pourrait être la raison de ce ralentissement subis. Nous avons aussi observer que le paramètre t avait une influences exponentielles sur le temps mis par le programme pour résoudre le puzzle au fur et a mesure que la clé de chiffrement s'agrandissait.

References

[1] *C++*. URL: hhttps://fr.wikipedia.org/wiki/C%2B%2B (visited on 01/09/2021).