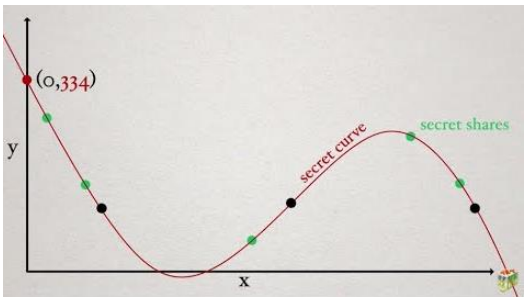
Matthieu Roux
Kevin Arguello
Besnik Emini

Shamir secret Sharing

Pour le projet de cours mathématiques 632-2, nous nous sommes penchés sur le projet de « Shamir's Secret Sharing ». Ce logiciel écrit en Java, est un algorithme permettant le partage de secret en multiple parts distinctes et unique à chaque ayant droit. L'idée de se partage, est de définir un nombre minimum de parts de secret à rentrer dans le logiciel afin de révéler le secret initial convoité.

Vue que ces codes sont basés sur les points d'une courbe de polynôme et qu'elle en possède à l'infini, on peut dire que le logiciel peut assigner des parts de secrets à ne plus savoir quoi en faire.

Pour que l'entreprise définisse le degré du polynôme, elle doit définir le nombre de parts requises pour trouver le secret initial. Plus il faut de part pour reconstruire le secret plus le degré du polynôme sera grand. Ensuite pour trouver le secret il faudra juste trouver le la fonction « y » avec le « x » au point « 0 » en trouvant la fonction et remplaçant le x par zéro pour trouver le F(0).



Pour notre projet, une contrainte nous a été imposée quant à la génération des parts de secrets. Notre équipe a dû prendre en compte une génération particulière de code en texte pour un des codes partagés, lequel sera convertit en hexadécimal avec padding pour permettre la conversion en nombre et et bouncy Castel pour crypter le texte puis ensuite qui sera converti en biginteger pour le sauvegarder dans un tableau de bits. Tout cette conversion va permettre d'associer le secret aux autres codes généré et le conserver dans le même format et dans un même emplacement.

Il faut savoir que la classe « UserService » est une méthode qui utilise le secret initial pour permettre la génération des parts pour les utilisateurs.

Pour la structuration de nos données, nous avons utiliser un format de données en Json pour conserver les codes et les enregistrer facilement afin de les utiliser d'une manière plus aisée.

La classe BigInteger offre des opérations de calcul en arithmétique modulaire afin de calculer le plus grand dénominateur commun pour les utiliser dans le shamir secret.

Matthieu Roux
Kevin Arguello
Besnik Emini

Manuel de l'utilisateur :

L'utilisation de l'application « Shamir's Secret Sharing » est assez simple à comprendre vue que les options s'offrent à l'utilisateur au moment du lancement de la classe « main ».

Dans la première option l'outil propose à l'utilisateur de créer (générer) le secret initial, qui va permettre dans les autres étapes basées sur ce secret, de générer les autres parts. L'utilisateur va devoir demander en quelle nombre de bits veut-il faire l'encodage. Il va devoir aussi écrire dans le texte que l'application devra convertir en hexadécimal et autre afin de le mettre au même format que les autres parts de secret.

Le nombre de part de secret pour reconstruire le secret initial sera également demandé afin de connaitre le degré du polynôme pour permettre aux autres étapes de générer les bonnes quantités de parts.

Pour ce qui est de la deuxième option « créer des parts de secret », c'est cette dernière qui va permettre de générer les parts du secret initial créé. Cette deuxième « étape » va aussi demander le nombre total de secret à générer au total qui prendra comme point de la courbe du polynôme et qu'il cryptera pour pas permettre l'identification simple du polynôme. Sachant que le nombre minimum de part de secret pour connaitre le secret doit être moins que celui des parts totales générer pour tous les ayant droits.

La troisième option, sert à révéler un secret en permettant aux personnes ayant obtenu une part de code. Pour pouvoir retrouver le secret initial il va falloir entrer le nombre de parts minimum initialisé dans les première option de l'application et aussi intégrer les « users » associer à ces codes qui sont assigné aux codes on moment où le cryptage ce fait et surtout dès que les deux valeurs sont récupérer par le Json pour les répertorier.