Travail à domicile : Cryptographie

1. Partage du secret à Seuil :

Le partage du secret à seuil est un algorithme cryptographique. C'est une forme de partage de secret, où un secret est divisé en parties, donnant à chaque participant sa propre part unique ou certaines parts ou toutes les parts sont nécessaires pour reconstruire le secret.
Compter sur tous les participants pour combiner le secret peut être peu pratique, et donc parfois le schéma de seuil est utilisé où n'importe quel k des parties est suffisant pour reconstruire le secret d'origine.
Le partage de clés secrètes de Shamir est utilisé pour sécuriser l'accès à un secret (un fichier, un texte...) de manière distribuée, le plus souvent pour sécuriser d'autres clés de chiffrement.

Pour déverrouiller l'accès au secret via le partage de clés secrètes de Shamir, vous avez besoin d'un nombre minimum de parts réunies. C'est ce qu'on appelle le seuil, qui est utilisé pour indiquer le nombre minimum de parts nécessaires pour reconstituer le secret et déverrouiller l'accès.

2. Principe du partage de secret à Seuil (k, n) :

Formellement, l'objectif principal de partage du secret est de diviser certain secret **S** en **n** parts **Si….,Sn,** avec **k<n** de telle manière que :

1. La connaissance de **k** parts ou plus de **Si**, rend le calcul de **S** facile.
2. La connaissance de n'importe quelles **k-1** parts ou moins de **Si** laisse **S** complètement indéterminée.

Cen schéma est appelé schéma à seuil (k,n). Si **k=n** alors tous les participants doivent participer pour reconstruire le secret **S**.

3. Le schéma de partage du secret de Shamir :

L'idée essentielle du schéma de seuil d'Adi Shamir est que : 2 points sont suffisants pour définir une ligne, 3 points sont suffisants pour définir une parabole, 4 points pour définir une courbe cubique et ainsi de suite. C'est-à-dire qu'il faut **k** points pour définir un polynôme de degré **k-1**.

Le principe du partage du secret de Shamir (k,n) est de partager in secret S en n parts attribués au participants (P1, P2,……Pn). En utilisant un polynôme aléatoire de degré k-1 et des coefficients aléatoires.

Construction des parts : Supposons qu'on veut utiliser un schéma à seuil (k,n) pour partager le secret **S < P** (P prime), supposé être un élément dans un corps fini F_P.

- ✓ Choisir aléatoirement $k-1$ coefficients $a_1, \cdots, a_{k-1}$dans F, et poser $a_0 = \boldsymbol{S}$.
- ✓ Construire le polynôme $f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_{k-1} x^{k-1} \, mod \, p$.

Distribution : Les couples de points sont distribués secrètement aux participants **Pn**.

- ✓ Soient n'importe quels n points calculés à partir de lui, par exemple $i = 1, \cdots, n$ qui donne $(i\,, f(i))$.
- ✓ Chaque point $(i\,, f(i))$ est attribué à un participant.

Reconstruction du secret :

- ✓ Etant donné n'importe quel k sous- ensemble de ces couples $(i\ , f(i))$ parmi n, on peut trouver les coefficients du ce polynôme à l'aide de l'interpolation de Lagrange et le secret soit le terme constant a_0.

$f(\mathrm{x}) = \sum_{i=1}^{n} y_i \cdot l_i \ mod\ p$ where: $l_i(\mathrm{x}) = \prod_{\substack{j=1 \\ x \neq j}}^{n} \frac{xj}{xj-xi}$

4. Example :

L'exemple suivant illustre l'idée de base. Notez, cependant, que les calculs dans l'exemple sont effectués en utilisant l'arithmétique des corps finis Fp

4.1 Préparation :

- Partage du secret de Shamir (k, n) = (3,5)
- Supposons que le secret $S = 11$, P=17.
- On souhaite partager le secret en 5 parts ($n = 5$), ou chaque sous-ensemble de 3 participants k=3 est suffisant pour reconstruire le secret. Aléatoirement, on choisit deux coefficients : $a_1 = 8, a_2 = 7$.
- Le polynôme pour produire des parts secrètes est :
  $f(x) = 11 + 8x + 7x^2\ mod\ p$

4.2 Construction des parts secrètes :

- On distribue les parts yi au participants P1, P2, P3, P4, P5.
  $y1 = 11 + 8(1) + 7(1)^2\ mod\ 17 = 9\ mod\ 17$
  $y2 = 11 + 8(2) + 7(2)^2\ mod\ 17 = 4\ mod\ 17$
  $y3 = 11 + 8(3) + 7(3)^2\ mod\ 17 = 13\ mod\ 17$
  $y4 = 11 + 8(4) + 7(4)^2\ mod\ 17 = 2\ mod\ 17$
  $y5 = 11 + 8(5) + 7(5)^2\ mod\ 17 = 5\ mod\ 17$

- On distribue les parts sur les participants :
- $P1: (x_1 y_1) = (1,9); P2: (x_{2,} y_2) = (2,4); P3: (x_{3,} y_3) = (3,13), P4: (4,2); P5: (5,5).$

4.3 Reconstruction des parts secrètes :

- Pour reconstruire le secret, on choisit 3 parts de 5 :

$P1: (x_1 y_1) = (1,9); P2: (x_{2,} y_2) = (2,4); P3: (x_{3,} y_3) = (3,13)$

- On calcule l'Interpolation de Lagrange :

$$S = y1\left(\frac{x_2}{x_2 - x_1} * \frac{x_3}{x_3 - x_1}\right) + y2\left(\frac{x_1}{x_1 - x_2} * \frac{x_3}{x_3 - x_2}\right) + y3\left(\frac{x_1}{x_1 - x_3} * \frac{x_2}{x_2 - x_3}\right)$$

$$S = 9\left(\frac{2}{2-1} * \frac{3}{3-1}\right) + 4\left(\frac{1}{1-2} * \frac{3}{3-2}\right) + 13\left(\frac{1}{1-3} * \frac{2}{2-3}\right)$$

$$S = 9(3) + 4(-3) + 13\,(1)\ mod\ 17 = 11$$

Exercice :

Un conseil d'administration prend ses décisions au moyen de votes électroniques. Il comporte un président dont la voix compte double et trois membres dont la voix est simple (notés 1, 2, 3). Une décision n'est prise que si un vote rassemble au moins 3 voix. Les votes sont acquis lorsque le titulaire présente selon son rang soit une soit deux parts d'un secret.

- Les services de sécurité ont fait implanter la méthode de Shamir avec une arithmétique modulo 31.
- Le secret partagé est tiré aléatoirement à la valeur 7.
- Les coefficients aléatoires du polynôme retenu sont 1, 9, et le terme constant est 7.
- On déduit les parts de secret du président des valeurs aux points x=1 ; x=2.
- On déduit des parts du secret des membres 1, 2, 3 des valeurs du polynôme pour 3, 4, 5.

1) Ecrire une fonction ShamirShare (s, k, n) qui retourne les valeurs des parts du secret partagé. Sachant que le s est le secret, le k est le seuil et le n est le nombre de tous les participants

2) Ecrire une fonction ShamirReconstruct qui reconstruit le secret s à partir des trois voix simples et à partir de la voix double du président et une voix simple d'un autre membre.

3) En utilisant les deux fonctions, écrire un script qui partage le secret donné et le reconstruire.