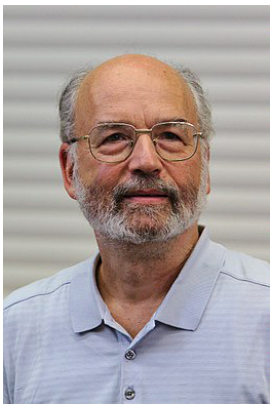
Théorie des codes - TP 7
ZZ3 F5 - Réseaux et Sécurité Informatique
Cryptographie distribuée : Partage de clé secrète de Shamir



Adi Shamir

Adi Shamir, né le 6 juillet 1952 à Tel Aviv, est un mathématicien et un cryptologue israélien reconnu comme l'un des experts les plus éminents en cryptanalyse. Il est principalement connu pour être le « S » de RSA créé avec Ron Rivest et Len Adleman datant de 1978. Mais, c'est loin d'être sa seule contribution au domaine de la cryptographie : il est à l'origine de la cryptanalyse du système de Merkle-Hellman , la technique de la cryptanalyse différentielle et l'auteur du protocole d'authentification sans apport de connaissance (Zero-knowledge).
De plus, il est à l'origine du **protocole de partage de clé secrète** qui porte son nom, basé sur la transmission d'une clé secrète par le biais de points construits sur un polynôme. La clé est ensuite retrouvée en utilisant l'interpolation de Lagrange.

Partage de secret de Shamir

L'algorithme de partage d'un secret de Shamir (1978) est un algorithme qui divise un secret en parts (*shares*). Le secret peut être récupéré en combinant un certain nombre de parts.
Imaginez un cas où vous devez chiffrer des données. Quelle que soit la méthode de chiffrement utilisée, vous devez stocker la clé secrète pour pouvoir déchiffrer ultérieurement et elle doit donc être très sécurisée. Si la clé est volée par un attaquant, vos données seront facilement décryptées par du simple déchiffrement. Cependant, retrouver la clé de stockage est toujours un problème difficile. Cela devient encore plus difficile si vous devez partager la clé avec d'autres. Ce problème de séquestre de clefs est source de maux de tête pour les administrateurs.
Clarifions certains termes utilisés dans le partage secret de Shamir :

- *Secret* : Le secret est un message secret ou un numéro que vous souhaitez partager avec d'autres en toute sécurité ;
- *Parts* : Le secret est divisé en morceaux et chaque morceau est appelé une part. Il est calculé à partir d'un secret donné. Afin de récupérer le secret, vous devez obtenir un certain nombre de parts ;
- *Seuil* : Le seuil est le nombre de parts dont vous avez besoin au moins pour récupérer votre secret. Vous pouvez restaurer votre secret uniquement lorsque vous accès à un nombre de parts supérieur ou égal au seuil.

Durant cette séance, nous allons implémenter l'algorithme de partage de clef sécrète de Shamir.

1. Dans un premier temps, vous allez mettre en place l'algorithme de Shamir (cf. annexe 1) où l'on pourra régler le nombre maximal d'utilisateurs n ainsi que le seuil k. Vous réaliserez des essais pour partager le secret ainsi que de le reconstruire avec k ou plus parts.

2. Dans un second temps, vous allez rajouter des fonctionnalités sur l'algorithme :
   - Sans changer les parts déjà données, l'algorithme devra pouvoir donner une nouvelle part à la demande ;
   - Sans changer les parts déjà données, l'algorithme devra pouvoir modifier le seuil k.

Appendix 1 Shamir's secret-sharing scheme

Introduction : [1] The essential idea of Adi Shamir's threshold scheme is that 2 points are sufficient to define a line, 3 points are sufficient to define a parabola, 4 points to define a cubic curve and so forth. That is, it takes k points to define a polynomial of degree $k-1$.
Suppose we want to use a (k,n)-threshold scheme to share our secret S without loss of generality assumed to be an element in a finite field F of cardinal P (we consider exponenent in $\mathbb{Z}/P\mathbb{Z}$) where $0 < k \leq n < P$; $S < P$ and P is a prime number.
Choose at random $k-1$ positive integers $a_1, \cdots, a_{k-1}$ with $a_i < P$, and let $a_0 = S$. Build the polynomial $f(X) = a_0 + a_1X + a_2X^2 + a_3X^3 + \cdots + a_{k-1}X^{k-1}$. Let us construct any n points out of it, for instance set $i = 1, \ldots, n$ to retrieve $(i, f(i))$. Every participant is given a point (a non-zero integer input to the polynomial, and the corresponding integer output) along with the prime which defines the finite field to use. Given any subset of k of these pairs, we can find the coefficients of the polynomial using interpolation. The secret is the constant term $f(0) = a_0$.

Algorithm : Shamir's algorithm consists of two parts :
- Share Computation ;
- Secret Reconstruction.

Algorithm 1 Share Computation

Require: given an prime number p, a number of user n and a thershold k
1: Decide secret : First, decide our secret message : S.
2: Create polynomial : Choose any numbers for coefficient, but the degree of the polynomial must be $k-1$.
3: **for** i = 1 ; i < k ; ++i **do**
4: Generate randomly : a_i
5: **end for**
6: The polynom is $P(X) = a_{k-1}X^{k-1} + \cdots + a_1X + S$
7: Create shares : for each users with the login x_i compute the share $y_i = P(x_i)$
8: **for** i = 1 ; i < k ; ++i **do**
9: Compute $P(x_i)$
10: **end for**
11: **return** Send the share to each user with a confidential transmission : $(x_i; y_i)_{i=1\cdots n}$

For example : Suppose that our secret is 1234 ($S = 1234$).
We wish to divide the secret into 6 parts ($n = 6$), where any subset of 3 parts ($k = 3$) is sufficient to reconstruct the secret. At random we obtain $k-1$ numbers : 166 and 94. $(a_0 = 1234; a_1 = 166; a_2 = 94)$, where a_0 is secret.
Our polynomial to produce secret shares (points) is therefore : $f(X) = 1234 + 166X + 94X^2$.
We construct 6 points $D_i = (i, f(i))$ from the polynomial :
$D_1 = (1, 1494)$; $D_2 = (2, 1942)$; $D_3 = (3, 2578)$; $D_4 = (4, 3402)$; $D_5 = (5, 4414)$; $D_6 = (6, 5614)$
We give each participant a different single point (both i and $f(i)$ and do not use $(0, f(0)$ because $f(0)$ is the secret).

1. *Extract of* `https://en.wikipedia.org/wiki/Shamir%27s_Secret_Sharing`

Algorithm 2 Secret Reconstruction

Require: k shares or more : $(x_i; y_i)_{i=1\cdots k}$

1: Compute the Lagrangian polynomials in zero $L_i(0)$
2: **for** i = 1 ; i < k ; ++i **do**
3: Compute $\alpha_i = L_i(0) = \prod_{j \neq i} \frac{x_j}{x_j - x_i}$
4: **end for**
5: **return** The secret S is $P(0) = \sum_{i=1}^{k} \alpha_i \times y_i$

For example : In order to reconstruct the secret any 3 points will be enough.
Let us consider $(x_0, y_0) = (2, 1942)\,; (x_1, y_1) = (4, 3402)\,; (x_2, y_2) = (5, 4414)$.
We will compute Lagrange basis polynomials :

$$\ell_0 = \frac{x - x_1}{x_0 - x_1} \cdot \frac{x - x_2}{x_0 - x_2} = \frac{x-4}{2-4} \cdot \frac{x-5}{2-5} = \frac{1}{6}x^2 - \frac{3}{2}x + \frac{10}{3}$$

$$\ell_1 = \frac{x - x_0}{x_1 - x_0} \cdot \frac{x - x_2}{x_1 - x_2} = \frac{x-2}{4-2} \cdot \frac{x-5}{4-5} = -\frac{1}{2}x^2 + \frac{7}{2}x - 5$$

$$\ell_2 = \frac{x - x_0}{x_2 - x_0} \cdot \frac{x - x_1}{x_2 - x_1} = \frac{x-2}{5-2} \cdot \frac{x-4}{5-4} = \frac{1}{3}x^2 - 2x + \frac{8}{3}$$

Therefore

$$f(x) = \sum_{j=0}^{2} y_j \cdot \ell_j(x)$$

$$= y_0\ell_0 + y_1\ell_1 + y_2\ell_2$$

$$= 1942(\frac{1}{6}x^2 - \frac{3}{2}x + \frac{10}{3}) + 3402(-\frac{1}{2}x^2 + \frac{7}{2}x - 5) + 4414(\frac{1}{3}x^2 - 2x + \frac{8}{3})$$

$$= 1234 + 166x + 94x^2$$

Recall that the secret is the free coefficient, which means that $S = 1234$, and we are done.