

## 3

## UN SECRET PARTAGÉ EN MORCEAUX

Il est possible de partager un message  $M$  en  $n$  morceaux  $M_1, M_2, \dots, M_n$  de telle façon que l'on n'ait aucune information sur  $M$  tant que l'on ne dispose pas de tous les  $n$  morceaux. Expliquons comment. On suppose  $M$  donné sous forme binaire et ayant la longueur  $L$ .

Pour  $M_1, M_2, \dots, M_{n-1}$ , on prend des suites de 0 et de 1 aléatoires, différentes et indépendantes, chacune de longueur  $L$ . Pour définir  $M_n$ , on procède bit par bit.

Pour le premier bit de  $M_n$ , on prend un 0 ou un 1 de façon que le nombre de 1 en première position dans les messages  $M_1, M_2, \dots, M_n$  soit pair si le premier bit de  $M$  est 0, et impair sinon.

Pour le deuxième bit de  $M_n$ , on procède de la même façon à partir des bits en deuxième position de  $M$  et de  $M_1, M_2, \dots, M_{n-1}$ . Et ainsi de suite (la procédure est illustrée ci-dessous pour  $n = 10$ , sur un message court).

Connaître  $M_1, M_2, \dots, M_n$  permet de reconstituer  $M$ , mais connaître  $n - 1$  de ces messages ne donne aucune information sur  $M$ .

On peut faire mieux et partager un message  $M$  en  $n$  morceaux de telle façon que :

– connaître  $k$  morceaux, quels qu'ils soient ( $k < n$ ), redonne  $M$  ;

– connaître moins de  $k$  morceaux ne donne aucune information sur  $M$ . Plusieurs méthodes ont été proposées, dont celle d'Adi Shamir (« How to share a secret », *Communications of the ACM*, vol. 22(11), pp. 612-613, 1979).

Son idée repose sur le fait que disposer de  $k$  valeurs d'un polynôme  $P$  de degré  $k - 1$  permet de le déterminer, mais que c'est impossible si l'on en connaît moins.

Le premier bit de  $M$  étant  $d_1$ , on commence par trouver un polynôme  $P_1$  de degré  $k - 1$  dont la valeur en 0 est  $d_1$ . Ensuite, pour chaque  $i$  de 1 à  $n$ , on fixe comme premier élément du message  $M_i$  la valeur  $P_1(i)$ .

On fait de même avec le second bit  $d_2$  de  $M$  : on choisit un polynôme  $P_2$  de degré  $k - 1$  dont la valeur en 0 est  $d_2$ . Puis, pour chaque  $i$  de 1 à  $n$ , on fixe comme second élément du message  $M_i$  la valeur  $P_2(i)$ . Et ainsi de suite.

En conséquence :

– celui qui connaît  $k$  messages parmi  $M_1, M_2, \dots, M_n$  connaîtra le 1<sup>er</sup> bit de  $M$ , car il peut calculer le polynôme  $P_1$ . Il connaîtra le 2<sup>e</sup> bit de  $M$ , car il peut calculer le polynôme  $P_2$ . Etc.  
– celui qui connaît moins de  $k$  messages parmi  $M_1, M_2, \dots, M_n$  ne peut rien connaître de  $M$ .

$M_1$ : 0100101011  
 $M_2$ : 1110011010  
 $M_3$ : 0010100111  
 $M_4$ : 0010110010  
 $M_5$ : 1101010011  
 $M_6$ : 1000101010  
 $M_7$ : 0100101001  
 $M_8$ : 1101001101  
 $M_9$ : 0111001000

$M$ : 0111001000

$M_{10}$ : 0110111001

> programmé fera l'affaire: vous délivrerez le message à la date voulue.

Ces méthodes sont intéressantes, mais uniquement pour des délais assez courts ne dépassant pas quelques mois ou années, car les batteries du téléphone ou de l'ordinateur caché doivent tenir jusqu'au moment du déclenchement. Elles ne permettent pas d'envoyer un message un siècle à l'avance.

De plus, les solutions avec téléphone ou ordinateurs cachés ne produisent pas un fichier informatique qu'on laisse circuler et qui est tel que tous ceux le détenant à l'heure voulue en découvrent le message sans avoir à interagir avec autre chose. Elles ont aussi l'inconvénient d'être lourdes à mettre en œuvre, sans parler du risque que le dispositif caché soit découvert et arrêté ou détruit par accident. Réfléchissons à mieux.

## FAIRE APPEL À UN OU PLUSIEURS TIERS DE CONFIANCE

Une idée évidente est celle du tiers de confiance. Vous confiez le message, placé dans une enveloppe cachetée par exemple, à un huissier en lui indiquant la date à laquelle il devra ouvrir l'enveloppe et en délivrer le contenu. Vous pouvez améliorer la robustesse du procédé en utilisant plusieurs tiers de confiance dont aucun ne pourra divulguer seul le message avant l'instant choisi par vous. Voici la méthode.

Vous découpez le message en  $n$  morceaux dont aucun ne permet d'avoir la moindre idée du message complet et dont même la connaissance de  $n - 1$  morceaux ne révèle rien (voir l'encadré 3). Vous confiez ces  $n$  morceaux à  $n$  tiers de confiance en leur demandant de se contacter les uns les autres à la date voulue pour s'échanger les bouts du message, le reconstituer et le rendre public.

Le risque sera cependant que l'un des tiers de confiance soit indisponible le jour voulu, malade ou décédé par exemple. Cela empêcherait que le message soit reconstitué et délivré. Mais il existe des procédés de découpage d'une information, inventés en 1979 par Adi Shamir et George Blakley, qui résolvent le problème. Le message est découpé en  $n$  morceaux qui ont la propriété que dès que l'on dispose de  $k$  morceaux ( $k < n$ ) du découpage, il devient possible de retrouver tout le message, et qu'avec moins de  $k$  morceaux, rien ne peut être dévoilé du message découpé (voir l'encadré 3).

Ces idées résolvent sans doute un certain nombre de cas, mais, comme précédemment, ce ne sont que des méthodes partiellement satisfaisantes: elles ne produisent pas une capsule temporelle, c'est-à-dire un message qui libère seul son information à la date voulue à ceux qui le détiennent.

Explorons d'autres idées. Ronald Rivest