HOW TO SHARE A SECRET

Maurice Mignotte, Strasbourg

I. Introduction.

We consider the following problem.

Let S be some secret. A collection of n people E_j share this secret in such a way that

- each E_j knows some information x_j,
- for a certain fixed integer k, $2 \leq k \leq n$, the knowledge of any k of the x's enables to find S easily,
- the knowlegde of less than k of the x's leaves S undetermined.

This problem was considered first by A. Shamir [79] and he calls such a scheme a (k, n) threshold scheme.

The practical interest of this problem is obvious and is discussed in Shamir [79].

Shamir gives a solution using interpolation of polynomials over a finite field, the secret being some polynomial. We give here a more elementary solution in which the secret is an integer. These two solutions are particular cases of the use of the Chinese Remainder Theorem. So we study this theorem in the following section.

II. Chinese Remainder Theorem.

Our problem is to cut some secret into pieces. An usual way in mathematics to "divide" a set into simpler pieces is to replace it by a product of simpler sets. A typical example of this situation is given by the

T. Beth (Ed.): Cryptography - EUROCRYPT '82, LNCS 149, pp. 371-375, 1983.

Chinese Remainder Theorem. Moreover, and this is essential in our application, the isomorphisms which occur in this theorem are easily computable for the two cases we consider.

The general version of the Chinese Remainder Theorem is the following.

THEOREM. - Let A be a ring. Let $I_1,\ldots,I_m$ be ideals of A such that

(1) $\quad I_j + I_{j'} = A \quad \text{for} \quad 1 \le j < j' \le m$.

Then, if $I = \bigcap_{j=1}^{m} I_j$, the function

$$\begin{aligned} f : A/I &\to A/I_1 \times \ldots \times A/I_m \\ x &\mapsto (x \bmod I_1, \ldots, x \bmod I_m) \end{aligned}$$

is an isomorphism of rings.

Moreover, if $z_1,\ldots,z_m \in A/I$ satisfy

$$z_i \equiv \delta_{ij} \bmod I_j \quad , \quad 1 \le i, j \le m$$

(where δ_{ij} = if $(i = j)$ then 1 else 0) then

$$f^{-1}(y_1,\ldots,y_m) = y_1 z_1 + \ldots + y_m z_m .$$

► Taking the product of relations (1) for $j = i$ and $j' \neq i$ we get

$$I_i + \bigcap_{\substack{1\le j\le m \\ j\neq i}} I_j = A \quad , \quad 1 \le i \le m .$$

The previous relation implies that there exist z'_i and z''_i , for $1 \le i \le m$, such that

$$1 = z'_i + z''_i \quad , \quad z'_i \in I_i \quad , \quad z''_i \in \bigcap_{\substack{1 \le j \le m \\ j \neq i}} I_j \,.$$

Then

$$z''_i \equiv \delta_{ij} \mod I_j \,.$$

If we put $z_i = z''_i \mod I$ and define

$$\begin{aligned} g : A/I_1 \times \dots \times A/I_m &\to A/I \\ (y_1, \dots, y_m) &\mapsto y_1 z_1 + \dots + y_m z_m \end{aligned}$$

it is easily verified that f and g are reciprocal homomorphisms. ◀

In our problem we take

secret : $S \in A/I$,

informations : $x_j = S \mod I_j$.

III. Shamir's example.

In our formulation, Shamir's solution can be seen as follows. He chooses $A = F[X]$, where $F = \mathbb{Z}/p\mathbb{Z}$ is a finite field (p is a prime member), and

$$I_j = \{Q \in F[X] \, ; \, Q(a_j) = 0\} \quad , \quad 1 \le j \le n$$

where $a_1, \dots, a_n$ are distinct points of F .
The secret is some polynomial $S \in F[X]$ of degree smaller than k and the x_j are

$$x_j = S(a_j) \quad , \quad 1 \le i \le n \,.$$

In this case the Chinese Remainder Theorem is the Legendre Theorem on interpolation of polynomials.

IV. An arithmetical solution.

We take now

- $A = \mathbb{Z}$,
- $I_j = d_j \mathbb{Z}$, $1 \leq j \leq n$, where $d_1, \ldots, d_n$ are coprime in pairs (the d's may be public)
- the secret is some integer S , $a \leq S \leq b$, where a and b are given integers, $0 < a < b$.
- the informations x_j are

$$x_j = S \bmod d_j \quad , \quad 1 \leq j \leq n .$$

To get a (k, n) threshold scheme we take $d_1, \ldots, d_n$ so that

- the product of any k of the d_j is bigger than b
- the product of any $k-1$ of the d_j is smaller than a .

When k of the x_j are known, say $x_1, \ldots, x_k$, then S is given by the formula

$$S = x_1 z_1 + \ldots + x_k z_k \mod d_1 \ldots d_k ,$$

and the z's are obtained by the (extended) euclidean algorithm. Moreover the z's have to be computed only once and one may take them so that

$$z_i \equiv \delta_{ij} \mod d_j \quad , \quad 1 \leq j \leq n$$

and then

$$S \equiv x_1 z_1 + \ldots + x_n z_n \mod d_1 \ldots d_n .$$

When only $k-1$ of the x_j are known, say $x_1, \ldots, x_{k-1}$ then

$$S \equiv x_1 z_1 + \dots + x_{k-1} z_{k-1} \mod d_1 \dots d_{k-1}$$

so that the interval $[a, b]$ contains at least $c = [\frac{b-a}{d_1 \dots d_{k-1}}]$ values which satisfy this condition and are equally possible values of S. If c is large enough (for example $c = 10^6$) then it is practically impossible to find S.

A possible choice is

- $d_j \simeq 10^{\ell}$, $1 \le j \le n$
- $a = 5.10^{k\ell-1}$, $b = 10^{k\ell}$,

where ℓ is some positive integer (for example $\ell = 6$).
Then when only $k-1$ or few of the x's are known there are at least about $5.10^{\ell-1}$ candidates for S.