# Impartirea secretelor

Împărțirea secretelor se referă la distribuirea unui secret între un grup de participanți cărora li se alocă o parte din mesaj, astfel că, acesta poate fi reconstituit numai atunci când un număr suficient de participanți(vom vedea mai tarziu care este acesta) își vor pune fiecare parte din secret la un loc. Fiecare parte din secret, independentă este practic inutilă, acestea furnizează informația necesară abia atunci cand puzzle-ul este refăcut(dupa o regulă dată, nefiind necesare toate piesele). Un alt avantaj al acestei scheme criptografice îl reprezintă faptul că nu necesită și stocarea unei chei(keyless). Modul în care dealer-ul împarte aceste părți din secret, poate fi unul ce depinde de gradul de încredere pe care îl are în persoana respectivă.

Există însă cazuri în care cheia este necesară și crește gradul de securitate. De exemplu: un dealer poate să împartă mai multe numere, ce inițial par a fi random, însă, după reconstruirea mesajului și decriptarea acestuia folosind o cheie, acesta poate fi decodificat într-un mesaj, compus din litere.

În unele situații există o cheie secretă care permite accesul la mai multe informații. Să presupunem că această cheie este pierdută(ori de persoana care o deține, ori dispozitivul pe care este stocată este distrus), atunci toate fișierele ce ar fi putut fi accesate cu acea cheie, au devenit acum indisponibile. O soluție pentru această problemă ar fi împărțirea cheii între mai multe entități, numite umbre(shadow) astfel încât cheia să poată fi aflată într-o submulțime de umbre.

Aceste scheme de împărțire a secretelor au fost descoperite de Blakley și Shamir.

**Împărtirea secretelor: Adi Shamir**

Principiul împartirii secretelor dezvoltat de Adi Shamir are la baza schema k din n sau (k, n) **threshold** (prag- numărul minim de părți din secret de care avem nevoie pentru a-l afla) cu 1 < k < n. Un dealer împarte secretul la n participanți. Astfel că, oricare k parți din mesaj pot reconstitui secretul, dar oricare k-1 parți din mesaj nu sunt suficiente. O astfel de schemă se numește perfectă dacă pentru orice grup de cel mult k-1 participanți nu poate afla mai multe informații despre secret decât o persoană din exteriorul grupului.

**Definiția matematică**

Fie un secret S. Pe acesta il divizam in n secrete: S1, …, Sn astfel incat:

1. Cunoasterea a cel putin k parti Si din mesaj duce la aflarea secretului S initial inainte de divizare => secretul poate fi reconstituit din oricare combinatie(submultime) de k sub-mesaje.
2. Cunoasterea a cel mult k-1 parti Si din mesaj nu ofera nicio informatie despre secretul integral => **securitatea perfecta**.

Exista si un caz in care k = n, astfel ca toate partile din mesaj sunt necesare pentru a-l reconstrui.

Ideea de baza a acestui algoritm consta in interpolarea polinomiala. Daca 2 puncte sunt suficiente si necesare pentru a defini o drepta, 3 puncte sunt pentru o parabola => un polinom de grad k – 1 este unic determinat de cei k coeficienti ai sai.

**Pas 1: Construirea “umbrelor”**

* Fie un numar prim p, p > max{S, n}, unde S este secretul, iar n este numarul de entitati intre care se imparte secretul.
* Apoi se aleg coeficientii astfel:
* a0 = S
* se aleg in mol aleatory k – 1 coeficienti independent a1, …, ak – 1 astfel incat 1 ≤ ai ≤ p – 1, 1 ≤ i ≤ k – 1.
* Cel care imparte secretul(dealer-ul) defineste urmatorul polinom cu coeficienti intr-un corp finit f =
* “Umbrele” secretului vor fi create dupa urmatoarea formula:

sj ≡ f(j) (mod p) (p este numar prim)

* Fiecare participant primeste perechea formata din (sj, j) printr-un canal sigur.

Pas 2: Reconstituirea secretului

Acum, ca un secret a fost impartit la n participant, presupunem ca la un moment dat este nevoie de secretul integral. Astfel, un grup de cel putin k personaje trebuie sa se reuneasca pentru a afla mesajul secret.

Fiecare pereche de tipul (j, sj) este considerata ca fiind un punct din plan (xi, yi) unde yj = f(xj). Pentru a afla functia polinomiala determinata de aceste puncte, se va folosi formula de interpolare Lagrange(sa explic ce inseamna aceasta interpolare – pe scurt).

**Formula pentru interpolarea Lagrange:**

Cum S = a0 = f(0) unde .

In concluzie, fiecare grup de k participant va determina valoarea secretului calculand o combinatie liniara(polinomul) a umbrelor. Coeficientii cj nefiind secreti.

Exemplu:

Pentru , graficul functiei polinomiale este o dreapta. Punctul A, in care dreapta intersecteaza axa Oy, are coordonatele (0, f(0)). Din S = f(0) => secretul este ordonata punctului A. Fiecare umbra este de fapt un punct pe dreapta. Cum am spus si mai sus, ca 2 puncte si suficiente si necesare pentru a determina o dreapta => oricare 2 puncte am alege pe dreapta, ele determina in mod unic dreapta => gasim astfel secretul.

Concluzie:

Deoarece schema lui Shamir este teoretic informational sigura, inseamna ca nici macar un atacator cu putere computationala nelimitata n-ar putea sa sparga aceasta schema. Ar putea face acest lucru doar daca ar intalni numarul minim necesar de persoane care detin cate o parte din secret.

Alte avantaje ale algoritmului lui Shamir sunt extensibilitatea si flexibilitatea => acesta poate adauga si alti participanti la impartirea secretului, dar fara sa modifica continutul original al mesaului.