**TEMA:** ALGORITMUL MERKEL-HELLMAN

Merkle-Hellman (MH) este unul dintre primele criptosisteme cu cheie publică, inventat de Ralph Merkle și Martin Hellman în 1978. Deși ideile de la baza acestuia sunt mai elegante și mai simple decât cele ale criptosistemului RSA, a fost spart. Sistemul Merkle-Hellman se bazează pe problema sumelor de submulțimi (un caz special al problemei rucsacului): dată o listă cu numere și un alt număr, care este suma unei submulțimi a listei de numere, determinați submulțimea. În general, această problemă este considerată a fi NP-completă; dar există niște cazuri ușoare care pot fi rezolvate eficient. Schema Merkle-Hellman este bazată pe transformarea unui caz ușor într-unul dificil, și invers. În orice caz, schema a fost spartă de Adi Shamir, nu prin atacarea problemei rucsacului, ci prin coruperea conversiei de la rucsacul ușor la cel dificil.

Algoritmul de cifrare Merkle-Hellman const˘a ˆın codificarea mesajului ca o solu¸tie a unei probleme de tip rucsac pentru care ponderile {M1, ..., Mn} constituie cheia de cifrare, ¸si

Σn

textului clar {b1, ..., bn} ˆıi corespunde textul cifrat

biMi.

i=1

Un ¸sir de ponderi {M1, ..., Mn} se nume¸ste supercresc˘ator dac˘a:

k−1

Σ

Mk > Mi pentru orice k.

i=1

Problema rucsacului supercresc˘ator este u¸sor de rezolvat folosind urm˘atoarea schem˘a: pentru k = n, ..., 1:

* + - dac˘a Mk < S atunci bk = 1 ¸si S = S − Mk;
    - altfel bk = 0.

Algoritmii de tip rucsac care nu sunt supercresc˘atori nu sunt u¸sor de rezolvat ¸si nu exist˘a nici un algoritm rapid care s˘a rezolve problema. Singura modalitate cunoscut˘a de a determina dac˘a bi = 1 const˘a ˆın testarea tuturor solu¸tiilor. Cei mai rapizi algoritmi de testare au o complexitate exponen¸tial˘a.

Algoritmul Merkle-Hellman se bazeaz˘a pe aceast˘a proprietate: cheia privat˘a este ¸sirul ponderilor pentru un rucsac supercresc˘ator iar cheia public˘a este ¸sirul ponderilor pentru un rucsac care are aceea¸si solu¸tie, dar nu este supercresc˘ator. Merkle ¸si Hellman au g˘asit o metod˘a prin care se poate transforma o problem˘a a rucsacului supercresc˘ator ˆıntr-o problem˘a normal˘a a rucsacului. Tehnica de conversie face apel la aritmetica modular˘a.

Avˆand la dispozi¸tie o problem˘a de tip rucsac supercresc˘ator (cheia privat˘a) cu ponderile M1, ..., Mn atunci aceasta se transform˘a ˆıntr-o problem˘a de tip rucsac normal˘a (cheia public˘a) cu ¸sirul ponderilor

{ }

{mM1 mod p, ..., mMn mod p},

unde m ¸si p sunt numere naturale prime ˆıntre ele (acestea fac parte din cheia privat˘a) ¸si

Σn

p >

Mi.

i=1

Pentru a cifra un mesaj binar acesta se va ˆımp˘ar¸ti ˆın blocuri de lungimi egale cu cardinalul

mul¸timii ponderilor. Cifrarea unui bloc b1...bn va fi num˘arul natural:

bi(mMi mod p).

Pentru descifrare destinatarul mesajului cunoa¸ste cheia privat˘a: ponderile originale ¸si valorile lui m ¸si p. Acesta va calcula mai ˆıntˆai pe m−1 mod p. Se va multiplica apoi textul cifrat cu m−1 mod p iar dup˘a aceea se va rezolva problema rucsacului supercresc˘ator pentru a recupera textul original.

**SCENARIU:**

S˘a se construiasc˘a cheia public˘a pentru algoritmul Merkle-Hellman reprezen- tat de

cheia privat˘a 2, 3, 6, 13, 27, 52 , modulul p = 105 ¸si multiplicatorul m = 31. Cifra¸ti mesajul 101110.

**Rezolvare:**

Avand la dispozi¸tie cheia privat˘a {M1, ..., Mn}, cheia public˘a se ob¸tine astfel

{mM1 mod p, ..., mMn mod p}.

Prin urmare, cheia privat˘a pentru datele de mai sus este {31·2 mod 105, 31·3 mod 105, 31· 6 mod 105, 31 · 13 mod 105, 31 · 27 mod 105, 31 · 52 mod 105} adic˘a {62, 93, 81, 88, 102, 37}.

Σn

Cifrarea mesajului 101110 ((m1, ..., m6)) se face dup˘a formula

i=1

mi(mMi mod p), adic˘a

pe baza cheii publice. Rezultatul va fi 62 + 81 + 88 + 102, deci mesajul cifrat este c = 333.

Ideea decriptării este determinarea lui s = r-1 (mod q). s este cheie privată în acest criptosistem. Acum se poate converti problema NP-completă, extrapolând α din c (utilizând un rucsac umplut aleator), într-o problemă ușoară de extrapolare a lui α folosind un rucsac supercrescător, care este rezolvabilă în timp liniar.

Pașii decriptării necesită calcularea lui c = c\*s (mod q) și w = β\*s (mod q).

Elementul c este încă o formă criptată a lui α, dar rucsacul care îl criptează este doar o secvență supercrescătoare, w. Problema rucsacului supercrescător este simplă de rezolvat datorită structurii unei secvențe supercrescătoare. Luați cel mai mare element din w, să zicem wk. Dacă wk > c, atunci αk = 0, dacă wk≤c, atunci αk = 1. Atunci, scădeți wk \* αk din c, și repetați acești pași până când obțineți α.

Când q este destul de mare, este foarte greu să se calculeze s (poate lua mult timp, dar algoritmul face apel la multiplicarea modulară). Dificultatea aflării lui s este faptul pentru care acest criptosistem a fost considerat imposibil de spart.

Decriptarea:S˘a se descifreze mesajul C = 4608 cifrat cu ajutorul algoritmului Merkle- Hellman

cu urm˘atorii parametrii: n = 9, cheia privat˘a 1, 2, 5, 10, 19, 40, 98, 179, 355 , mod- ulul p = 1717 ¸si multiplicatorul m = 507.

Rezolvare: Se determin˘a C m−1 mod 1717 = 4608 507−1 mod 1717 = 4608 657 mod

· · ·

1717 = 385.

Apoi se rezolv˘a problema supercresc˘atoare a rucsacului de dimensiune 385 : 385 = 355 + 19 + 10 + 1. Mesajul clar va con¸tine 1 pe pozi¸tiile corespunz˘atoare acestor ponderi, deci se ob¸tine 100110001.