Criptosisteme cu cheie publică

Una din probleme criptosistemelor simetrice este aceea a distribuţiei cheilor şi a menagementului lor. Dacă Alice şi Bob folosesc un astfel de criptosistem, trebuie să schimbe o cheie secretă înainte de a putea comunica. Pentru schimbul cheilor ei au nevoie de un canal sigur sau chiar de un curier. Problema schimbului de chei devine chiar mult mai dificilă dacă mai multe persoane vor să schimbe mesaje criptate, de exemplu pe Internet. Dacă o reţea de comunicaţie are n utilizatori şi oricare dintre ei schimbă o cheie, atunci sunt necesare $n(n-1)/2$ schimburi de chei, şi toate acestea trebuie păstrate secret. O altă posibilitate pentru schimbul cheilor este aceea ca fiecare utilizator să schimbe o cheie secretă cu un centru de stocare al cheilor. Dacă Alice vrea să trimită un mesaj lui Bob, atunci ea criptează mesajul folosind cheia sa secretă şi îl trimite centrului de chei. Centrul, cunoscând toate cheile secrete, decriptează mesajul folosind cheia lui Alice, îl criptează din nou cu cheia lui Bob, şi-l trimite lui Bob. În acest fel numărul de schimburi de chei se reduce la n. Totuşi, centrul de chei va şti toate mesajele secrete şi trebuie să stocheze toate cheile secrete.

Pentru a rezolva aceste probleme au fost introduse *criptosistemele cu chei publice* (public key cryptosystems). În acest caz menagementul cheilor este mult mai simplu. Într-un sistem cu chei publice doar cheile de decriptare trebuie ţinute secret. O cheie de decriptare se numeşte *cheie secretă* sau *cheie privată*. Cheia de criptare corespunzătoare poate fi făcută publică şi se numeşte *cheie publică*. Cheia privată nu poate fi obţinută din cheia publică. Aceasta este proprietatea de bază a criptosistemelor cu cheie publică.

O schemă simplă de lucru este următoarea. Fiecare utilizator este listat într-un director public cu cheia sa publică. Dacă Alice vrea să trimită un mesaj lui Bob, ea obţine cheia publică a lui Bob din directorul public. Apoi foloseşte această cheie pentru a cripta mesajul şi-l trimite lui Bob. Acesta este acum în măsură să decripteze mesajul folosind cheia lui privată. Evident în acest caz şi Oscar poate trimite lui Bob mesaje cifrate şi de aceea se impune ca mesajele să aibă o aşa numită *signatură*, adică un fel de semnătură pentru ca Bob să ştie sigur de la cine primeşte mesajul. Deci fiecare când trimite mesaje lui Bob foloseste cheia sa, însă doar Bob va putea decifra mesajul. Tabelul trebuie păstrat sigur în sensul că toţi pot să-l vadă dar nu oricine poate scrie în el. Altminteri Oscar poate pune în tabel la Bob cheia sa şi prin urmare ar putea decifra toate mesajele primite de Bob.

În general criptosistemele cu chei publice sunt folosite pentru a fi trimise chei ce vor fi apoi folosite pentru a cripta cu criptosisteme simetrice, precum DES sau AES.

Criptosistemul ElGamal

- A fost introdus de Taher ElGamal în 1985 în articolul "A public key cryptosystem and a signature scheme based on discrete logarithms".
- Este strâns legat de protocolul Diffie-Hellman de generare a unei chei comune secrete.
- Securitatea sistemului se bazează pe dificultatea rezolvării problemei logaritmului discret (sau a problemei Diffie-Hellman) în $\mathbb{Z}_p^*$

1. **Generarea cheilor**
   - Alice alege un număr prim p mare (aproximativ 770 biţi) şi un generator g al lui $G = (\mathbb{Z}_p^*, \cdot)$, $2 \leq g \leq p-2$.
   - Alice alege arbitrar un exponent $a \in \{0, \ldots, p-2\}$ pe care-l ţine secret şi calculează u, $1 \leq u < p$ prin
   $$u = g^a \bmod p.$$
   - Cheia publică a lui Alice este (p, g, u) (întregul u este partea de cheie a lui Alice din protocolul Diffie-Hellman)
   - Cheia secretă a lui Alice este a.
2. **Criptarea**
   - $M = \{2, \ldots, p-1\}$ este spaţiul textelor simple, şi fie $m \in M$ un text simplu pe care Bob vrea să-l trimită cifrat lui Alice.
   - Bob alege arbitrar un exponent $b \in \{0, \ldots, p-2\}$ (este secret şi "efemer" adică este folosit doar pentru criptarea unui singur mesaj) şi calculează întregul v, $1 \leq v < p$ astfel ca
   $$v = g^b \bmod p.$$
   - Bob calculează întregul c, $1 \leq c < p$
   $$c = u^b m \bmod p$$
   (cu alte cuvinte Bob face cifrarea înmulţind mesajul m cu cheia obţinută prin protocolul Diffie-Hellman)
   - Textul cifrat în criptosistemul ElGamal este (v, c).
3. **Decriptarea**
   - Alice primeşte mesajul cifrat (v, c) şi ştie cheia secretă a. Calculează numerele
   $$k = v^a (= g^{ab}) \bmod p$$
   şi
   $$k^{-1} \bmod p.$$
   - Alice calculează
   $$c \cdot k^{-1} = c \cdot (g^{ab})^{-1} = m \cdot (g^{ab}) \cdot (g^{ab})^{-1} = m \bmod p.$$

Observaţia 1. *Pentru a evita calculul inversului modular Alice calculează mai întâi întregul* $x = p - 1 - a$, $1 \leq x \leq p - 2$ *şi apoi* $m \equiv v^x \cdot c \bmod p$. *Să observăm că de fapt* m *este mesajul original, adică acest procedeu ne dă într-adevăr decifrarea mesajului:*

$$v^{p-1-a}c = g^{b(p-1-a)}u^b m = (g^{p-1})^b (g^a)^{-b} u^b m = u^{-b}u^b m = m \bmod p,$$

deoarece $g^{p-1} \equiv 1 \bmod p$ (g *are ordinul* $p - 1$).

Exemplul 1. *Alice alege numărul prim* $p = 23$ *şi generatorul* $g = 7$ *al lui* $G = (\mathbb{Z}_{23}^*, \cdot)$. *Apoi Alice alege numărul* $a = 6$ *pe care-l ţine secret şi calculează* u *prin* $u = 7^6 \equiv 4 \bmod 23$. *Cheia publică a lui Alice este* $(23, 7, 4)$ *Cheia secretă a lui Alice este* $a = 6$.

Bob vrea să-i trimită mesajul $m = 7$. *El alege* $b = 3$ *şi calculează* $v = g^b = 7^3 = 21 \bmod 23$ *şi* $c = u^b m = 4^3 7 = 11 \bmod 23$. *Textul cifrat trimis de Bob este deci* $(21, 11)$. *Alice îl decifrează prin* $v^{p-1-a}c = 21^{23-1-6}11 = 7 \bmod 23$.∎

Observaţii

- Dacă Oscar poate rezolva PLD atunci poate sparge sistemul ElGamal. Deoarece Oscar ştie (p, g, u, v), el poate calcula (de exemplu) $\log_g u = a$ şi apoi $m = v^{p-1-a} \cdot c \pmod p$.
- Rămâne încă o problemă deschisă dacă spargerea sistemului ElGamal implică şi rezolvarea PLD.
- Spargerea criptosistemului ElGamal este echivalentă cu rezolvarea problemei Diffie-Hellman.

  Presupunem că Oscar are un algoritm pentru problema Diffie-Hellman, adică poate construi cheia secretă $k = g^{ab} \bmod p$ cunoscând $\{p, g, u, v\}$. Atunci Oscar va decifra un text cifrat ElGamal (v, c), pentru că ştie cheia k (el ştie cheia publică (p, g, u) a lui Alice şi textul cifrat (v, c)) şi rămâne să calculeze doar $k^{-1}c \bmod p$.

  Reciproc, presupunem că Oscar poate sparge criptosistemul ElGamal. Atunci el poate găsi textul simplu m din $\{p, g, u, v, c\}$, adică poate decifra (v, c) cunoscând cheia publică a lui Alice. În particular pentru $c = 1$ el aplică acest algoritm şi obţine textul simplu corespunzător m. Dar din cifrare Oscar are $1 = km \bmod p$ şi deci, deduce $k = m^{-1} \bmod p$.
- Trebuie să remarcam că dacă Bob alege pentru două cifrări distincte acelaşi exponent b , să zicem $c = u^b m \bmod p$, $c' = u^b m' \bmod p$ atunci Oscar ştie că are loc $c'c^{-1} = m'm^{-1} \bmod p$. Dacă adiţional, Oscar ştie textul simplu m atunci aflarea lui m' este imediată. Deci, reţinem că este bine ca cifrarea să se facă de fiecare dată cu b distincţi.