Kako deliti skrivnosti

17. april, 2002

Danes že vsi vemo, da imajo informacije podobno, včasih celo večjo vrednost kot denar. Zato moramo biti pri dodeljevanju dostopa do njih skrajno previdni. Iz izkušenj vemo, da ni dobro povsem zaupati nobenemu posamezniku, še posebej, če je v njegovih rokah usoda mnogih. Vedno se tudi lahko zgodi, da je uporabnik neupravičeno izključen iz sistema (npr. če izgubi ključe) ali da nepooblaščeni uporabniki uspejo vdreti v sistem.

V prispevku bomo predstavili nekaj splošnih postopkov za deljenje skrivnosti. Le-ti sodijo med osnovne prijeme za povečanje zaupanja v delovanje informacijskih sistemov. To področje predstavlja enega izmed stebrov moderne kriptografije in je tesno povezano s skrbjo za varno in odgovorno ravnanje s ključi.

Za začetek si oglejmo nekaj zanimivih primerov deljenja skrivnosti.

> *Na tajnem projektu dela n oseb, materiali o projektu pa so spravljeni v trezorju z več ključavnicami. Dostop do materialov je dovoljen le tedaj, kadar se zbere večina, tj. več kot polovica oseb. Vsak sodelavec dobi enako število ključev. Koliko najmanj ključavnic je potrebno in koliko ključev mora dobiti vsak?*

Predno si pogledaš rešitev, morda poskusi rešiti nalogo za $n = 2, 3, 4, \ldots$, nato pa tvegaj z napovedjo, kaj bi utegnila biti dobra spodnja meja za število ključavnic.

Rešitev: Predpostavimo najprej, da nam je ključe uspelo razdeliti tako, kot zahteva naloga, in poglejmo kaj znamo ugotoviti o številu ključev. Naj bo $k = \lfloor (n+1)/2 \rfloor$ in $s = \binom{n}{k}$. Potem obstaja natanko s različnih k-elementnih podmnožic oseb, ki delajo na tajnem projektu: $G_1, G_2, \ldots, G_s$. Vsaka skupina G_i vsebuje vsaj $n/2$ oseb, zato osebe zunaj te skupine nimajo vseh ključev. Naj bo K_i množica ključev, ki jim manjkajo. Potem nobena izmed množic K_i, $i \in \{1, \ldots, s\}$, ni prazna. Skupaj s katerimkoli članom skupine G_i pa imajo vse ključe, torej ima vsaka oseba iz G_i vse ključe iz K_i. Naj bo $i \neq j$. V množici G_i obstaja oseba, ki ni v G_j. Ta oseba nima nobenega izmed ključev iz K_j, torej je $K_i \cap K_j = \emptyset$. Ker sta bila i in j poljubna, od tod sledi, da je različnih ključev vsaj s.

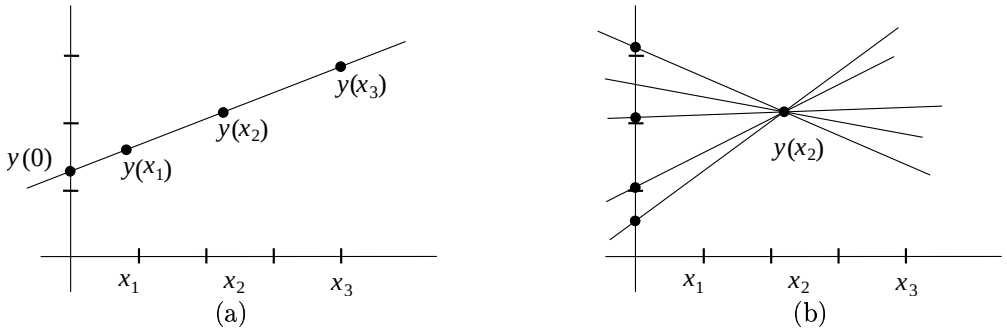
Sedaj pa pokažimo, da je s ključev $k_1, \ldots, k_s$, vedno tudi dovolj za rešitev zastavljene naloge. Ključe razdelimo tako, da dobijo ključ k_i natanko vse osebe iz skupine G_i. Tako dobi vsaka oseba $\binom{n-1}{k-1}$ ključev. Le večinska skupina ima neprazen presek z vsemi podmnožicami G_i, tako da lahko le taka skupina odpre trezor. ∎

Najprej smo ugotovili, da mora biti ključavnic vsaj s, nato pa smo našli način, kako dodeliti vsaki osebi $\binom{n-1}{k-1}$ ključev, tako da bodo lahko le večinske skupine odklenile vse ključavnice.

> *V banki morajo* **trije** *direktorji vsak dan odpreti trezor, vendar pa kombinacije ne želijo zaupati nobenemu posamezniku. Zato bi radi imeli sistem, po katerem lahko odpreta trezor poljubna* **dva** *med njimi.*

Zgornja rešitev nam svetuje ($n = 3$, $k = 2$, $s = \binom{3}{2} = 3$), da nastavimo na trezor tri ključavnice in damo vsakemu direktorju dva ključa (seveda pa nobenemu isti par). Vendar pa lahko v tem primeru vsak direktor odklene dve ključavnici in že s tem bistveno oslabi varnost, npr. za trikrat skrajša čas, potreben za odstranitev ključavnic.

Želimo najti rešitev, ki ne bo nikomur dala prednosti pred zunanjim vlomilcem. Ta problem lahko rešimo z $(2, 3)$-stopenjsko shemo za deljenje skrivnosti, glej sliko 1. Takšne sheme sta leta 1979 neodvisno odkrila **Blakley** in **Shamir**.



Slika 1: $(2, n)$-stopenjska shema za deljenje skrivnosti, $n \in \mathbb{N}$. Delivec si v ravnini izbere premico ℓ, ki ni navpična, in za vsako osebo na tej premici izbere svojo točko, ki ne leži na osi y. Za zgornji sliki si izberemo $n = 3$.
(a) Vsaka oseba dobi le koordinato y svoje točke, ki jo shrani na primer na pametni kartici. Program v trezorju pozna še ustrezne od 0 različne koordinate x, zato lahko izračuna ključ $y(0)$, ki je enak odseku, kjer premica ℓ seka os y. Vsaki dve točki natanko določata premico in s tem ključ.
(b) Če imamo eno samo točko, ne moremo ugotoviti, kateri ključ je pravi, saj so vsi videti enako dobri.

V Rusiji so v 90-ih letih prejšnjega stoletja uporabljali $(2, 3)$-stopenjsko shemo za kontrolo jedrskega orožja (predsednik, obrambni minister, vrhovni vojaški poveljnik).

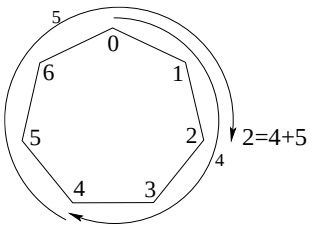
V splošnem je **(t, n)-stopenjska shema** za deljenje skrivnosti K med n oseb, $2 \leq t \leq n$, metoda, za katero velja:

- poljubnih t oseb lahko izračuna skrivnost K,
- nobena skupina s $t - 1$ (ali manj) osebami ne more izračunati prav nobene informacije o skrivnosti K.

Sheme za deljenje skrivnosti so vsestransko uporabne. Lahko jih uporabimo povsod, kjer do podatkov dostopamo hierarhično. Tak način dostopa je pogost v velikih podjetjih, bankah in vojski.

Če računamo z običajnimi tipi števil, ki so na voljo v standardnih programskih jezikih, moramo rezultate izračunov zaradi omejene velikosti teh tipov nenehno zaokrožati (posebno ko postajajo števila vse večja in večja ali pa jih delimo). V kriptografiji pa približki ne

zadoščajo, zato si za računanje raje omislimo končne množice kot pri številčnici na uri. Tak zgled so kolobarji $\mathbb{Z}_n$, $n \in \mathbb{N}$, v katerih računamo po modulu števila n. Za elemente vzamemo $\{0, 1, \ldots, n-1\}$, računamo pa tako, da seštejemo ali zmnožimo dve števili tako, da pravi rezultat nadomestimo z njegovim ostankom pri deljenju z *modulom* n. Na primer za $n = 7$ velja $4 + 5 \mod 7 = 2$ in $5 \cdot 4 \mod 7 = 6$, saj ima vsota 9 ostanek 2 pri deljenju s 7, produkt 20 pa ostanek 6, glej sliko 2.



Slika 2: Računanje po modulu 7.

Videli smo že, kako z geometrijskim argumentom zasnujemo $(2, n)$-stopenjsko shemo za deljenje skrivnosti. Poglejmo sedaj, kako skonstruiramo (t, t)-stopenjsko shemo za deljenje skrivnosti:

*(1) Naj bo m neko dovolj veliko naravno število ($m \geq t + 1$), $K \in \mathbb{Z}_m$ (**skrivnost**) in $\mathcal{P} = \{P_1, \ldots, P_t\}$ množica oseb, ki jim želimo razdeliti skrivnost.*

(2) Delivec $D \notin \mathcal{P}$ neodvisno izbere naključna števila $y_1, y_2, \ldots, y_{t-1} \in \mathbb{Z}_m$ in izračuna

$$y_t = K - (y_1 + \cdots + y_{t-1}) \mod m.$$

(3) Oseba P_i dobi del y_i, $1 \leq i \leq t$.

Osebe $P_1, \ldots, P_{i-1}, P_{i+1}, \ldots, P_t$ lahko izračunajo samo $K - y_i$, kar pa jim nič ne pomaga, saj je bilo število y_i naključno izbrano, medtem ko vsi skupaj samo seštejejo svoje dele in dobijo skrivnost K.

Shamir je skonstruiral splošno (t, n)-stopenjsko shemo za deljenje skrivnosti za poljubni naravni števili t in n, $2 \leq t \leq n$. Za tako shemo je dovolj, da v $(2, n)$-stopenjski shemi za deljenje skrivnosti nadomestimo premico s polinomom stopnje $t-1$, saj je tak polinom določen s t točkami.

Spomnimo se, da je **polinom** spremenljivke x definiran s predpisom

$$f(x) = a_0 + a_1 x + \cdots + a_n x^n, \qquad a_i \in \mathcal{O},$$

kjer je $\mathcal{O}$ nek obseg (npr. $\mathbb{R}$ ali pa $\mathbb{Z}_p$, p praštevilo). **Ničla** polinoma f je taka vrednost $a \in \mathcal{O}$, za katero je $f(a) = 0$.

V praštevilskih kolobarjih $\mathbb{Z}_p$, kjer je p praštevilo, je možno tudi deljenje z vsakim od 0 različnim elementom $a \in \mathbb{Z}_p$ in zato tudi sodijo med obsege. Deljenje je namreč kar množenje z recipročnim elementom. Če le-tega označimo z x, potem velja $a \cdot x \mod p = 1$, zato ga lahko poiščemo kot rešitev diofantske enačbe $ax + py = 1$ z razširjenim Evklidovim algoritmom (glej članek M. Juvana, O Evklidovem algoritmu, *Presek* **21** (1993-94), str. 116–121). Ta enačba je vedno rešljiva, saj sta si a in p tuja.

Izrek 1: *Od nič različen polinom stopnje n ima v obsegu največ n ničel.*

Zgornji izrek ne velja vedno, če koeficienti polinoma niso iz obsega. Na primer v kolobarju $\mathbb{Z}_6$ zgornja trditev ne drži, saj ima kvadratni polinom $f(x) = (x-1)x$ kar štiri ničle: $0, 1, 3, 4$. Za prvi dve ničli potrebujemo prisotnost le po enega faktorja, za zadnji dve pa potrebujemo hkrati oba faktorja. V obsegih pa je produkt lahko nič le tedaj, ko je vsaj en izmed faktorjev enak nič. Če je a ničla polinoma f, potem nam razcep $x^i - a^i = (x-a)(x^{i-1} + \cdots + a^{i-1})$ zagotavlja, da lahko zapišemo $f(x) = f(x) - f(a) = (x-a)q(x)$, kjer je q polinom stopnje $n-1$. Torej se nam za vsako ničlo, ki jo izpostavimo, zmanjša stopnja preostanka za 1 in zato število ničel res ne more preseči stopnje polinoma.

*(1) Naj bo p neko dovolj veliko praštevilo ($p \geq n+1$), $K \in \mathbb{Z}_p$ (**skrivnost**) in $\mathcal{P} = \{P_1, \ldots, P_n\}$ množica oseb, ki jim želimo razdeliti skrivnost.*

(2) Delivec $D \notin \mathcal{P}$ izbere n različnih elementov $x_1, x_2, \ldots, x_n \in \mathbb{Z}_p \backslash \{0\}$ in dodeli del x_i osebi $P_i \in \mathcal{P}$ (vrednosti x_i so lahko javne).

(3) Za delitev ključa K delivec D naključno in neodvisno izbere $t-1$ elementov $a_1, \ldots, a_{t-1} \in \mathbb{Z}_p$ ter za $i = 1, \ldots, n$ izračuna $y_i = a(x_i)$, kjer je

$$a(x) = K + a_1 x + \cdots + a_{t-1} x^{t-1} \bmod p,$$

in da del y_i osebi P_i.

Primer: Naj bo $p = 17$, $t = 3$ in $n = 5$. Za javne koordinate x izberimo $x_i = i$, $1 \leq i \leq 5$. Predpostavimo, da osebe P_1, P_3 in P_5 združijo svoje dele, ki so zaporedoma enaki 8, 10 in 11. Če vzamemo $a(x) = a_0 + a_1 x + a_2 x^2$ in izračunamo $a(1)$, $a(3)$ ter $a(5)$, dobimo sistem treh linearnih enačb v $\mathbb{Z}_{17}$:

$$\begin{aligned} a_0 + a_1 + a_2 &= 8, \\ a_0 + 3a_1 + 9a_2 &= 10, \\ a_0 + 5a_1 + 8a_2 &= 11, \end{aligned}$$

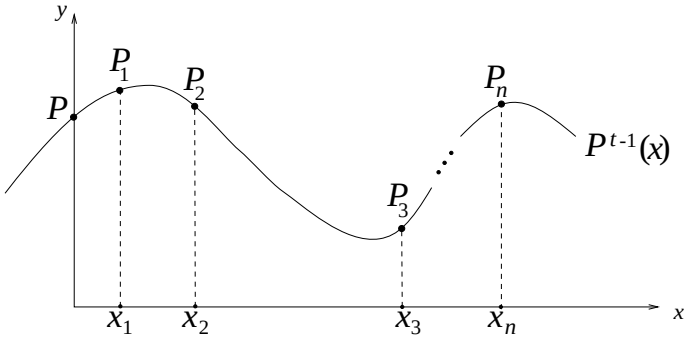
ki ima v $\mathbb{Z}_{17}$ enolično rešitev $a_0 = 13$, $a_1 = 10$ in $a_2 = 2$. Ključ je torej enak $K = a_0 = 13$.

V primeru splošne Shamirjeve sheme osebe $P_1, P_2, \ldots, P_t$ določijo ključ K iz enačb:

$$y_i = a(x_i) = a_0 + a_1 x_i + \cdots + a_{t-1} x_i^{t-1}, \qquad \text{za } 1 \leq i \leq t.$$

S pomočjo metod, ki močno presegajo srednješolsko matematiko, lahko z matrikami in determinantami pokažemo, da ima ta sistem enolično rešitev v $\mathbb{Z}_p$. Drugi način pa je, da si pomagamo s polinomom $p(x)$ stopnje največ $t-1$, ki ga zna izračunati vsaka skupina t oseb iz svojih delov. Poznamo ga pod imenom **interpolacijski polinom** (glej sliko 3) in ga vpeljemo prek polinomov $p_i(x) = (x-x_1)(x-x_2)\cdots(x-x_{i-1})(x-x_{i+1})\cdots(x-x_t)$, tj. produktov faktorjev $(x-x_j)$ za $j \neq i$:

$$p(x) = y_1 \frac{p_1(x)}{p_1(x_1)} + \cdots + y_t \frac{p_t(x)}{p_t(x_t)}.$$



Slika 3: Interpolacijski polinom.

Faktor v i-tem sumandu ob y_i zavzame vrednost 1 za $x = x_i$ in 0 za vsak drug x_j. Z neposrednim računom ugotovimo, da velja $p(x_i) = a(x_i)$, $i = 1, \ldots, t$. Od tod sledi, da ima polinom $p(x) - a(x)$, ki je stopnje kvečjemu $t-1$, vsaj t ničel. Izrek 1 nam potem zagotovi, da je to možno le, kadar sta polinoma $a(x)$ in $p(x)$ enaka. Zato je $K = p(0)$.

Da se prepričamo, da je to res (t, n)-stopenjska shema za deljenje skrivnosti, moramo utemeljiti še, da $t-1$ oseb ne more izključiti nobenega ključa. Če k $t-1$ osebam (te poznajo $t-1$ delov skrivnosti) dodamo za poljuben $a_0 \in \mathbb{Z}_p$ še del $y_0 = a_0$, ki predstavlja vrednost polinoma $a(x)$ v točki $x_0 = 0$, potem z zgornjo formulo zopet dobimo polinom $a(x)$, ki ustreza vsem podatkom, ki so trenutno na voljo.

Ko želi skupina t oseb izračunati ključ K iz svojih delov, pravzaprav ne potrebuje celotnega polinoma $p(x)$, pač pa samo vrednost:

$$K = y_1 \frac{p_1(0)}{p_1(x_1)} + \cdots + y_t \frac{p_t(0)}{p_t(x_t)}.$$

Od tod se lepo vidi, da je iskani ključ linearna kombinacija delov y_i: $K = b_1 y_1 + b_2 y_2 + \cdots + b_t y_t$, kjer je

$$b_i = \frac{p_i(0)}{p_i(x_i)} = \frac{x_1 x_2 \cdots x_{i-1} x_{i+1} \cdots x_t}{(x_1 - x_i)(x_2 - x_i) \cdots (x_{i-1} - x_i)(x_{i+1} - x_i) \cdots (x_t - x_i)},$$

torej je bila (t, t)-stopenjska shema za deljenje skrivnosti le poseben primer splošne sheme. Še več, za samo uporabo splošne sheme za deljenje skrivnosti v resnici ne potrebujemo ne računanja interpolacijskih polinomov ne reševanja sistemov enačb, temveč le seštevanje, množenje in deljenje v končnem obsegu.

Nadaljevanje primera: Osebe P_1, P_3 in P_5 lahko izračunajo b_1, b_3, b_5 po zgornji formuli. Če izračunamo recipročne elemente z razširjenim Evklidovim algoritmom, dobimo:

$$b_1 = \frac{x_3 x_5}{(x_3 - x_1)(x_5 - x_1)} \bmod 17 = 3 \cdot 5 \cdot 2^{-1} \cdot 4^{-1} \bmod 17 = 4.$$

Podobno izračunamo tudi $b_3 = 3$ in $b_5 = 11$ ter za dele 8, 10 in 11 dobimo

$$K = 4 \cdot 8 + 3 \cdot 10 + 11 \cdot 11 \bmod 17 = 13.$$

Za konec poudarimo, da je varnost Shamirjeve sheme za deljenje skrivnosti *brezpogojna*, tj. noben ključ ni na podlagi informacij, ki jih imajo nepooblaščene množice, bolj verjeten

od drugega. Možne so seveda še razne posplošitve, kot je dodelitev različnih prioritet različnim osebam (npr. za dostop do vojaške skrivnosti sta potrebna dva generala ali pet majorjev) ipd., a to je že druga zgodba. Prav tako spadajo v posebno zgodbo tudi kriptosistemi, ki so odvisni od računsko zahtevnih problemov, kot je na primer faktorizacija števil (šifrirne sheme RSA) ali pa diskretni logaritem (ElGamalovi kriptosistemi in digitalni podpis DSA). Več o deljenju skrivnosti si radovedni bralec lahko poišče v učbeniku D.R. Stinsona, Cryptography – Theory and Practice, CRC Press, 1995 ali pa na moji domači strani (`http://valjhun.fmf.uni-lj.si/~ajurisic/`).

Aleksandar Jurišić