

Kryptografia s verejným kľúčom

4. januára 2003

- veľká požiadavka po flexibilnej kryptografii vyžaduje nové prístupy
- hlavnou nevýhodou klasickej kryptografie je, že musíte poslať dlhý kľúč super tajným kanálom
- pri symetrickej kryptografii museli mať obaja účastníci rovnaký kľúč
- kryptografia s verejným kľúčom má dve rozdielne kľúče pre komunikujúce strany
- ak nie je možné zo znalosti kryptovacieho algoritmu zostrojiť dekryptovací - potom môže byť kryptovací alg. verejný
- je nutné cez verejný kanál vytvoriť tajný kľúč

Diffie a Hellman

1. Alica aj Bob sa dohodnú na prvočísle p a primitívnym koreňom $q \pmod{p}$
2. Alica si vyberie náhodné číslo x : $1 \leq x \leq p - 1$
3. Alica vypočíta X : $X = q^x \pmod{p}$
4. Bob si vyberie náhodné číslo y : $1 \leq y \leq p - 1$
5. Bob vypočíta Y : $Y = q^y \pmod{p}$
6. Alica s Bobom si vymenia X a Y (verejným kanálom)
7. Alica a Bob si nechajú tajné x a y
8. Alica spočíta $Y^x \pmod{p}$
9. Bob spočíta $X^y \pmod{p}$
 - Obaja poznajú kľúč: $K = q^{xy} \pmod{p}$
 - Eva by musela vypočítať diskretný logaritmus na prelomenie

Útok man in the middle

1. Eva si vyberie z
2. Eva zachytí q^x a q^y
3. Alici a Bobovi pošle q^z - obaja veria, že dostali to čo chceli
4. Spočíta kľúče: $K_A = q^{zx} \pmod{p}$ a $K_B = q^{zy} \pmod{p}$
 - Ak príde správa od Alice - dešifruje ju kľúčom K_A , prečíta a zašifruje kľúčom K_B . Túto správu pošle Bobovi. Takto si môže prečítať správy bez toho, aby niekto vedel, že komunikácia nie je bezpečná

Blom - distribúcia kľúčov

- dôveryhodná autorita Trent môže distribuovať $n(n-1)/2$ kľúčov medzi n komunikujúcich účastníkov
 - verejne je známe prvočíslo $p > n$
1. každému užívateľovi je priradené jednoznačné identifikačné číslo $r_U < p$
 2. Trent si vyberie 3 náhodné čísla a, b, c (menšie než p)
 3. Pre každého užívateľa U , Trent spočíta: $a_U = (a + br_U) \bmod p$ a $b_U = (b + cr_U) \bmod p$
 4. odošle a_U a b_U užívateľovi U cez zabezpečený kanál
 5. každý užívateľ si vytvorí polynom $g_U(x) = a_U + b_U x$
 6. Ak chce Alica komunikovať s Bobom, tak spočíta: $K_{AB} = g_A(r_B)$ a Bob: $K_{BA} = g_B(r_A)$
- poznámka: $K_{AB} = K_{BA}$

Komunikácia bez dôveryhodnej autority

- každý užívateľ X má svoju vlastnú šifrovaciu a dešifrovaciu funkciu - e_X a d_X
 - funkcie sú komutatívne
1. Alica pošle Bobovi: $e_A(w)$
 2. Bob pošle Alici: $e_B(e_A(w))$
 3. Alica pošle Bobovi: $d_A(e_B(e_A(w)))$
 4. Bob dešifruje: $d_B(d_A(e_B(e_A(w))))$ a dostane w
- príliš náročná komunikácia
 - distribúcia kľúčov je perfektná

Jednocestná funkcia

- $F : N \rightarrow N$
- $x \rightarrow F(x)$ je výpočet jednoduchý
- $F(x) \rightarrow x$ nie je výpočet jedoducho realizovateľný (napr. v polynomiálnom čase)

Silne jednocestná funkcia

- f je vypočítateľná v polynomiálnom čase
- pravdepodobnosť výpočtu $f^{-1}(f(x))$ náhodnostným algoritmom je menšia než $\frac{1}{n^c}$ (c je konštanta a n je horná hranica?)
- $f(x) = a^x \bmod n$
- $f(x) = x^2 \bmod n$ (kde n je Blumovo číslo)
- $f(p, q) = pq$ (násobenie prvočísla)

Funkcia so zadnými vrátkami

- f a f^{-1} sa dá spočítať jednoducho
- znalosť algoritmu pre výpočet f neumožňuje vypočítať f^{-1}
- umocňovanie s pevným modulom

Batôžkový problém

- Merkle a Hellman
 - super rastúci vektor - suma predchádzajúcich hodnôt je menšia
 - kódovanie: $c = Ab^T$ - A je superrastúci vektor, b^T je transponovaný bitový vektor
 - dekódovanie: od c sa postupne odčítavajú zložky vektora od najväčšej po najmenšiu, ak je zvyšok po odčítaní menší než nasledujúca zložka - potom sa preskakuje a odčítava sa až ďalšia zložka, ktorá je väčšia než aktuálna hodnota c
 - ak nie je vektor superastúci, môže dôjsť k dešifrovaniu kryptotextu na dva (príp. viac) plaintexty
1. vytvoriť superastúci vektor $X(x_1 \dots x_n)$
 2. vybrať m, u : $m > 2x_n$, $\gcd(m, u) = 1$
 3. spočítať $u^{-1} \bmod m$
 4. vytvoriť nový vektor: $X' = (x'_1 \dots x'_n)$, kde $x'_i = ux_i \bmod n$
 - difúziu hodnôt predstavuje násobenie konštantou u
 - konfúziu (zmätenie) predstavuje operácia mod
 - X' je verejný kľúč
 - X, u, m predstavujú zadné vrátka
 - šifrovanie je násobenie vektoru verejného kľúča binárnym vektorom: $c = X'w$
 - dešifrovanie: $c' = u^{-1}c \bmod n$ a výpočet batôžkového problému s X a c'
 - iterovaný batôžkový problém s hyper-reachable vektorom - zmena je v $m > 2\sum_{i=1}^n x_i$
 - ďalšou možnosťou na sťaženie rozlomenia je využitie hustoty (dense knapsack)

McEliece

- využíva Goppa kódy - lineárne ktoré je možné dešifrovať v polynomiálnom čase
- Goppa: $[2^m, n - mt, 2t + 1]$
- G je generujúca matica $k \times n$ pre $[n, k, d]$
- S je náhodná binárna matica $k \times k$ invertovateľná v \mathbb{Z}_2
- P je náhodná permutačná matica $n \times n$
- $G' = SGP$
- G' je verejný kľúč
- G, S, P predstavujú súkromný kľúč
- šifrovanie a dešifrovanie je pekne zložité
- pri kódovaní sa zanašajú do kódu chyby, ktoré sú opraviteľné použitím Goppa kódu
- nie je však bezpečné šifrovať dvakrát ten istý plaintext

Kľúče

- master key - hlavný kľúč, ktorý je veľmi dobre strážený
- session key - kľúč vygenerovaný pomocou master key a je určený len na jednu reláciu