Teorija kodiranja in kriptografija 2013/2014

Kriptosistemi z javnim ključem - problem diskretnega logaritma

Arjana Žitnik

Univerza v Ljubljani, Fakulteta za matematiko in fiziko

Ljubljana, 1. 4. 2014

Vsebina

- Problem diskretnega logaritma
- Diffie-Hellmanova izmenjava ključev
- El-Gamalov kriptosistem

Kriptosistemi z javnim ključem

Varnost kriptosistema z javnim ključem ponavadi temelji na predpostavki, da je določen matematični problem težko rešiti.

V razvoju javne kriptografije je bilo predlaganih in razbitih veliko kriptosistemov. Le nekaj se jih je obdržalo in jih lahko danes štejemo za varne in učinkovite. Delimo jih glede na matematični problem, na katerem temeljijo:

- Faktorizacija celih števil (na primer RSA),
- Problem diskretnega logaritma (na primer DSA)
- Problem diskretnega logaritma na eliptični krivulji

Problem diskretnega logaritma v grupi G

DLP: Naj bo G multiplikativna grupa.
za dana $\alpha, \beta \in G$, kjer je red elementa α enak n,
je treba poiskati takšen $x \in \{0, \ldots, n-1\}$, da je

$$\alpha^x = \beta,$$

če tak x obstaja.

Število x imenujemo diskretni logaritem elementa β z osnovo α.

Medtem ko je diskretni logaritem (verjetno) težko izračunati (v splošnem), lahko potenco izračunamo hitro.

Problem diskretnega logaritma v grupi $\mathbb{Z}_p^*$

Za dana $\alpha, \beta \in \mathbb{Z}_p^*$, kjer je red elementa α enak $p-1$, je treba poiskati takšen $x \in \{0, \ldots, p-2\}$, da je

$$\alpha^x = \beta \pmod{p}.$$

Opomba:
Problem diskretnega logaritma v grupi $(\mathbb{Z}_p, +_p)$ se glasi

Za dana $\alpha, \beta \in \mathbb{Z}_p$, kjer je red elementa α enak p, je treba poiskati takšen $x \in \{0, \ldots, p-1\}$, da je

$$\alpha \cdot x = \beta \pmod{p}.$$

Ta problem hitro rešimo z razširjenim Evklidovim algoritmom!

Algoritmi za računanje diskretnega logaritma

- Shankov algoritem (veliki korak – mali korak),
- Pollardov ρ-algoritem,
- Pohlig-Hellmanov algoritem,
- metoda “index calculus”.

Če je red grupe enak n, prvi trije algoritmi poiščejo diskretni logaritem v času $\mathcal{O}(\sqrt{(n)})$.

Pohlig-Hellmanov algoritem prevede problem iskanja DL v grupi na problem iskanja v ciklični podgrupi, zato je boljše, če je n praštevilo.

Zadnja metoda je subeksponentna, deluje pa le na grupah $GF(q)^*$.

Razlogi za uporabo različnih grup

- operacije v nekaterih grupah so izvedene enostavneje v programih (software) in programski opremi (hardware) kot v drugih grupah,
- problem diskretnega logaritma je lahko v določeni grupi zahtevnejši kot v drugi (na primer, v grupi točk na eliptični krivulji metoda index calculus ne deluje, zato lahko uporabimo krajše ključe).

ElGamalovi protokoli

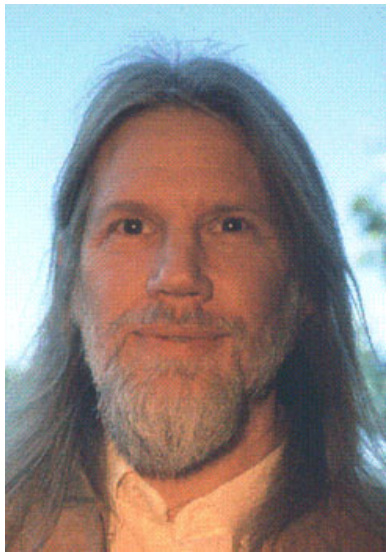
Delimo jih v tri razrede:

1. protokoli za izmenjavo ključev,
2. kriptosistemi z javnimi ključi,
3. digitalni podpisi.

ElGamalove protokole lahko uporabimo s poljubno končno grupo G, njihova varnost temelji na zahtevnosti problema diskretnega logaritma.

Diffie-Hellmanova izmenjava ključev

Za začetek kriptografije z javnimi ključi štejemo leto 1976, ko sta Whitfield Diffie in Martin Hellman našla odgovor na vprašanje, kako se lahko dve osebi preko javnega kanala dogovorita o skupnem ključu, ki bo znan le njima.



Whitfield Diffie

Martin Hellman

Diffie-Hellmanova izmenjava ključev

1. Alenka in Bojan se dogovorita za veliko praštevilo p ($p \geq 2^{1024}$) in za $\alpha \in \mathbb{Z}_p^*$, ki ima velik red n.
2. Alenka si izbere naključno število $a \in \{1, 2, \ldots, n-1\}$, izračuna $A = \alpha^a \pmod{p}$ in pošlje A Bojanu.
3. Bojan si izbere naključno število $b \in \{1, 2, \ldots, n-1\}$, izračuna $B = \alpha^b \pmod{p}$ in pošlje B Alenki.
4. Alenka in Bojan vsak zase izračunata skupni tajni ključ $K = \alpha^{ab}$:
   - Alenka izračuna: $B^a = (\alpha^b)^a = \alpha^{ab} = K$.
   - Bojan izračuna: $A^b = (\alpha^a)^b = \alpha^{ab} = K$.

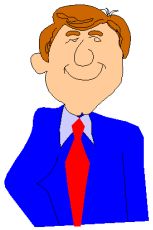
Diffie-Hellmanova izmenjava ključev - slika

Alenka izbere a
in izračuna $A=\alpha^a$

Bojan izbere b
in izračuna $B=\alpha^b$

A

B



Alenka izračuna

$K=B^a=\alpha^{ba}$

Bojan izračuna

$K=A^b=\alpha^{ba}$

Varnost DH izmenjave ključev

Varnost temelji na težavnosti Diffie-Hellmanovega problema: nasprotnik ne more hitro izračunati ključa

$$\alpha^{ab},$$

če pozna le

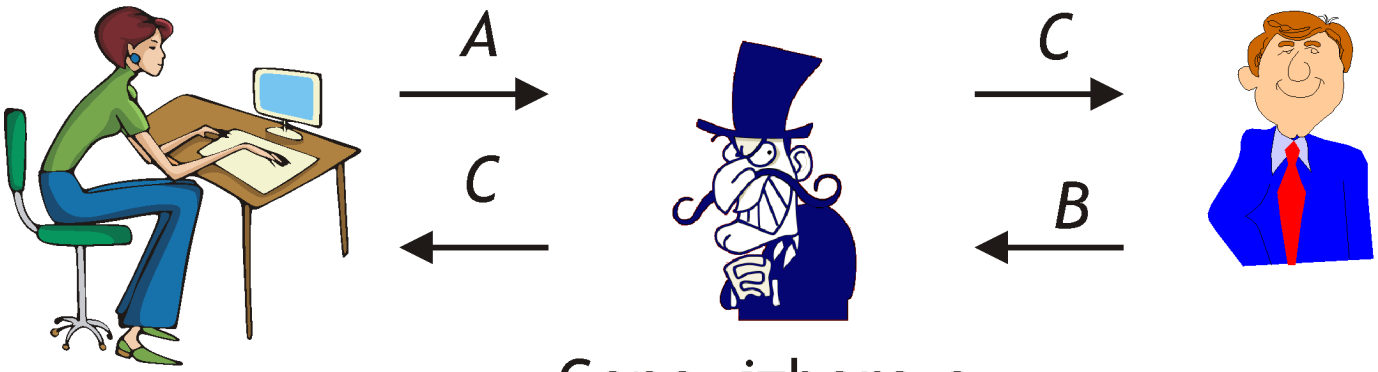
$$\alpha^{a}, \quad \alpha^{b} \text{ in } \alpha.$$

Če lahko hitro izračunamo diskretni logaritem, razbijemo tudi Diffie-Hellmanovo shemo.

Napad srednjega moža

Alenka izbere a
in izračuna $A=\alpha^a$

Bojan izbere b
in izračuna $B=\alpha^b$



Cene izbere c
in izračuna $C=\alpha^c$

Alenka deli skupni ključ $K1=\alpha^{ac}$ s Cenetom.

Bojan deli skupni ključ $K2=\alpha^{bc}$ s Cenetom.

Zaradi možnosti napada srednjega moža je pri izmenjavi ključa nujna avtentikacija!

ElGamalov kriptosistem (Taher ElGamal, 1985)

Ideja

1. Alenka in Bojan izmenjata tajni ključ k z Diffie-Hellmanovo shemo.
2. Alenka želi poslati Bojanu besedilo x.
   Izračuna kriptogram $y = k \cdot x \pmod{p}$
   in ga pošlje Bojanu.
3. Bojan izračuna $x = k^{-1} \cdot y \pmod{p}$.

ElGamalov kriptosistem - formalna definicija

Naj bo p praštevilo in α primitiven element v $\mathbb{Z}_p^*$.

Za ElGamalov kriptosistem je

- $\mathcal{B} = \mathcal{C} = \mathbb{Z}_p^*$
- $\mathcal{K} = \mathbb{Z}_p^* \times \mathbb{Z}_p^*$
- $E_{(a,B)}(x) \equiv B^a \cdot x \pmod{p}$
- $D_{(b,A)}(y) \equiv A^{p-b-1} \cdot y \pmod{p}$

Naj bo $B = \alpha^b \pmod{p}$ in $A = \alpha^a \pmod{p}$.
Potem kodirnemu ključu (a, B) ustreza dekodirni ključ (b, A).

ElGamalov kriptosistem - obrnljivost kodiranja

Preverimo:

$$
\begin{aligned}
D_{(b,A)}(E_{(a,B)}(x)) &\equiv D_{(b,A)}(B^a \cdot x) \pmod{p} \\
&\equiv A^{p-b-1} \cdot (B^a \cdot x) \pmod{p} \\
&\equiv (\alpha^a)^{p-b-1} \cdot (\alpha^b)^a \cdot x \pmod{p} \\
&\equiv \alpha^{a(p-1)-ab+ab} \cdot x \pmod{p} \\
&\equiv x \pmod{p}
\end{aligned}
$$

ElGamalov kriptosistem - uporaba

1. Bojan izbere: praštevilo p, generator α in število $b \in \{1, 2, \ldots, p-2\}$ ter
   izračuna: $B \equiv \alpha^b \pmod{p}$;
   Bojanov objavi svoj javni ključ: (p, α, B).

2. Alenka želi poslati Bojanu besedilo x.
   Alenka izbere naključen eksponent $a \in \{1, 2, \ldots, p-2\}$ ter
   izračuna: $A \equiv \alpha^a \pmod{p}$ in $y \equiv B^a \cdot x \pmod{p}$;
   Alenka pošlje Bojanu: (A, y).

3. Bojan dekodira: $A^{p-b-1} \cdot y \equiv x \pmod{p}$.

ElGamalov kriptosistem -zgled

1. Bojan izbere: $p = 2579$, $\alpha = 2$, $b = 765$;
   Bojan izračuna: $B = 2^{765} \equiv 949 \pmod{2578}$;
   Bojan objavi svoj javni ključ: $(p, \alpha, B) = (2579, 2, 765)$;

2. Sporočilo in naključen eksponent: $x = 1299$, $a = 853$;
   Alenka izračuna $A = 2^{853} \equiv 435 \pmod{2579}$;
   Kriptogram: $y = 949^{853} \cdot 1299 \equiv 2396 \pmod{2579}$,

3. Bojan dekodira:
   $435^{1813} \cdot 2396 = 1980 \cdot 2396 \equiv 1299 \pmod{2579}$.

ElGamalov kriptosistem - prednosti

- Naključnost: Alenka eksponent a vsakič naključno izbere. Zato je isto besedilo vsakič drugače kodirano, s čimer preprečimo napad z znanim besedilom (če napadalec pozna x_1 in y_1, lahko izračuna $B^a = y_1 \cdot x_1^{-1} \pmod{p}$ in potem za vse $i \geq 2$ dobi $x_i \equiv (B^a)^{-1} \cdot y_i \pmod{p}$).
- Pri izbiri parametrov lahko izberemo eksponent b, ki je tuj proti $p-1$. Potem je

$$B = \alpha^b \pmod{p}$$

tudi primitivni element v $\mathbb{Z}_p^*$:

$$(\alpha^b)^k \equiv 1 \pmod{p} \implies p-1 | bk \implies p-1 | k \implies \text{red}(\alpha^b) = p-1$$

To je ugodno, ker je potem slučajna spremenljivka B^a enakomerno porazdeljena na $\{1, 2, \ldots, p-1\}$.

- Uporabnost v vsaki grupi, kjer je potenciranje učinkovito, problem diskretnega logaritma pa težek.

ElGamalov kriptosistem - slabosti

- Dolžina sporočila se podvoji.
- Občutljivost na napad z znanim besedilom, če pošiljatelj "reciklira" eksponent a.
- Občutljivost za nadzorovano spreminjanje sporočila: nasprotnik lahko besedilo x spremeni v besedilo $x \cdot z \pmod{p}$, saj iz $y \equiv B^a \cdot x \pmod{p}$ sledi $y \cdot z \equiv B^a \cdot x \cdot z \pmod{p}$.
- Potrebna je avtentikacija: sporočilo lahko prebere le Bojan (s pomočjo svojega zasebnega ključa), ni pa rečeno, da mu ga je zares poslala Alenka, saj ni nikjer uporabila svojega zasebnega ključa.
- Varnost temelji na DH - problemu, ki je kvečjemu lažji kot problem diskretnega logaritma.

Primerjava simetričnih in asimetričnih kriptosistemov

	Simetrični sistemi	Asimetrični sistemi
Prednosti	hitrost kodiranja/dekodiranja	preprosta izmenjava ključev
Slabosti	težavna izmenjava ključev	počasnost kodiranja/dekodiranja

Hibridni kriptosistemi

Ideja: izberemo simetrični kriptosistem $\mathcal{S}$ (npr. AES) in asimetrični kriptosistem $\mathcal{A}$ (npr. RSA)

1. $\mathcal{A}$ uporabimo za izmenjavo ključa za sistem $\mathcal{S}$.
2. $\mathcal{S}$ uporabimo za kodiranje sporočila.

V praksi se uporabljajo predvsem hibridni sistemi.