Полиг-Хелман алгоритам

Владимир Божовић

Одсјек за математику
Природно-математички факултет

КРИПТОГРАФИЈА

Рјешавање линеарних конгруенција

Конгруенција

$$ax \equiv b \pmod{m}$$

има рјешења ако и само ако $d \mid b$ гдје је **нзд**$(a, m) = d$.
Рјешења добијамо у три корака:

1. Скрати се претходна конгруенција са d, па имамо

$$a'x' \equiv b' \pmod{m'}, \text{ одакле је } \textbf{нзд}(a', m') = 1.$$

2. Нека је x_0 јединствено рјешење претходне конгруенције (Еуклидов алгоритам).
3. Сва рјешења почетне конгруенције су дата са

$$x_0 + k\frac{m}{d}, \quad k = 0, 1, \ldots, d-1.$$

Кинеска теорема о остацима - начин размишљања

- Више од алгоритма и теореме, Кинеска теорема о остацима је заправо начин математичког размишљања.
- Ако је $m = m_1 m_2 \cdots m_t$ производ релативно простих бројева, онда Кинеска теорема о остацима каже да је, у принципу, рјешавање једначина модуло m, еквивалентно рјешавању система једначина са модулима m_i, за сваки i.

Кинеска теорема о остацима - начин размишљања

- Као што знамо, ДЛП се састоји у тражењу рјешења једначине
$$g^w \equiv h \pmod{p}.$$
- На први поглед, чини се да због чињенице да је p прост број, Кинеска теорема неупотребљива.
- Међутим, треба имати у виду да се рјешење x тражи по модулу $p-1$.
- Ово сугерише да **факторизација** $p-1$ може играти улогу у одређивању тежине датог ДЛП.

Кинеска теорема о остацима - начин размишљања

- Претходно можемо уопштити на произвољну групу G у којој рјешавамо проблем облика

$$g^w = h,$$

при чему рјешење тражимо у интервалу од 1 до N, гдје је N ред елемента g.

- Значи, питање факторизације N постаје од суштинског заначаја за рјешавање ДЛП-а.
- Ово је основна идеја на којој почива Полиг-Хелман алгоритам.

Кинеска теорема о остацима и Полиг-Хелман

Теорема

Нека је G група и претпоставимо да имамо алгоритам који рјешава ДЛП у G за неки елемент чији је ред степен простог броја. Конкретније, нека $a \in G$ има ред q^e, гдје је q прост број. Претпоставимо да одговарајући ДЛП $a^u = b$ можемо ријешити у $O(S_{q^e})$ корака. Нека је сада $g \in G$ елемент реда N и нека је

$$N = q_1^{e_1} q_2^{e_2} \cdots q_t^{e_t}$$

његова факторизација. Тада ДЛП $g^w = h$ може бити ријешен у

$$O\left(\sum_{i=1}^{t} S_{q_i^{e_i}} + \log(N)\right) \text{ корака.}$$

Кинеска теорема о остацима и Полиг-Хелман

Доказ претходне теореме изводимо у два корака:

1. За свако $1 \leq i \leq t$, нека је

$$g_i = g^{N/q_i^{e_i}} \text{ и } h_i = h^{N/q_i^{e_i}}.$$

Примјетимо да g_i има ред $q_i^{e_i}$, што је степен простог реда, па можемо користити дати алгоритам да ријешимо ДЛОГ

$$g_i^y = h_i. \qquad (*)$$

Нека је $y = y_i$ рјешење (*).

Кинеска теорема о остацима и Полиг-Хелман

2. Користимо Кинеску теорему о остацима за рјешавање система

$$x \equiv y_1 \pmod{q_1^{e_1}}, \ldots, x \equiv y_t \pmod{q_t^{e_t}}. \qquad (**)$$

Доказ Полиг-Хелман алгоритма

- Остаје да покажемо да се описаном процедуром заиста добија рјешење ДЛОГ-а $g^w = h$.
- Нека је s рјешење система конгруенција (**). Дакле,

$$s \equiv y_1 \pmod{q_1^{e_1}}, \ldots, s \equiv y_t \pmod{q_t^{e_t}}.$$

Онда је, за свако појединачно i, $1 \leq i \leq t$,

$$s = y_i + q_i^{e_i} z_i \text{ за неко } z_i. \qquad (***)$$

Доказ Полиг-Хелман алгоритма

Показујемо да вриједи

$$g_i^s = h_i,\ 1 \leq i \leq t.$$

Како је $s \equiv y_i \pmod{q_i^{e_i}}$, онда је $s = y_i + s_i q_i^{e_i}$, па је

$$\begin{aligned} g_i^s &= \left(g^{N/q_i^{e_i}}\right)^s = g^{(y_i + s_i q_i^{e_i})N/q_i^{e_i}} \\ &= g^{y_i N/q_i^{e_i}} \cdot g^{N s_i} = g^{y_i N/q_i^{e_i}} \\ &= \left(g^{N/q_i^{e_i}}\right)^{y_i} = g_i^{y_i} = h_i, \end{aligned}$$

за свако $1 \leq i \leq t$.

Доказ Полиг-Хелман алгоритма

Дакле, вриједи $g_i^s = h_i$, што значи

$$(g^s)^{N/q_i^{e_i}} = h^{N/q_i^{e_i}},\ 1 \leq i \leq t.$$

Са, друге стране, имамо да је $g^w = h$, па је

$$g^{sN/q_i^{e_i}} = g^{wN/q_i^{e_i}},\ 1 \leq i \leq t,$$

односно

$$s\frac{N}{q_i^{e_i}} \equiv w\frac{N}{q_i^{e_i}} \pmod{N},\ 1 \leq i \leq t. \qquad (***)$$

Доказ Полиг-Хелман алгоритма

На крају, потребно је уочити да је

$$\text{нзд}\left(\frac{N}{q_1^{e_1}}, \frac{N}{q_2^{e_2}} \ldots, \frac{N}{q_t^{e_t}}\right) = 1,$$

а потом и доказати да постоје цијели бројеви $c_1, c_2, \ldots, c_t$ тако да

$$c_1 \frac{N}{q_1^{e_1}} + c_2 \frac{N}{q_2^{e_2}} + \cdots + c_t \frac{N}{q_t^{e_t}} = 1.$$

Доказ Полиг-Хелман алгоритма

Сада, множењем обје стране (***) са c_i, за $1 \leq i \leq t$, а потом и сумирањем, добијамо

$$\sum_{i=1}^{t} c_i \frac{N}{q_1^{e_1}} s \equiv \sum_{i=1}^{t} c_i \frac{N}{q_1^{e_1}} w \pmod{N}.$$

Из претходног слиједи

$$s \equiv w \pmod{N},$$

што значи да је s заправо рјешење постављеног ДЛОГ-а.

Доказ Полиг-Хелман алгоритма

Како је цијена рјешавања појединачних ДЛОГ проблема у дијелу (1)

$$O\left(S_{q_i^{e_i}}\right), 1 \leq i \leq t,$$

а Кинеска теорема о остацима, у дијелу (2), кошта $O(\log(N))$ корака, онда је вријеме извршења алгоритма

$$O\left(\sum_{i=1}^{t} S_{q_i^{e_i}} + \log(N)\right).$$

Кинеска теорема о остацима и Полиг-Хелман

- Pohlig–Hellman алгоритам у принципу редукује ДЛП произвољног модула на ДЛП за модуло степена простих бројева. Следеће поједностављење ће овај проблем свести на ДЛП само по модулу простих бројева.

Разрада Полиг-Хелмана

Теорема

Нека је G група. Претпоставимо да је q прост број и претпоставимо да нам је познат алгоритам који у S_q корака рјешава ДЛП $g^x = h$ у G уколико g има ред q. Сада, нека је $g \in G$ произвољан елемент реда q^e гдје је $e \geq 1$. Тада је могуће ријешити ДЛП

$$g^x = h \text{ у } O(eS_q) \text{ корака .}$$

Разрада Полиг-Хелмана

Доказ претходне теореме се заснива на опсервацији да се x може записати у q-арном систему

$$x = x_0 + x_1 q + x_2 q^2 + \cdots + x_{e-1} q^{e-1}.$$

Из $h = g^x$, закључујемо

$$h^{q^{e-1}} = \left(g^{q^{e-1}}\right)^{x_0}.$$

Дакле, с обзиром на то да је ред елемента $g^{q^{k-1}}$ једнак q, претходни ДЛОГ се може ријешити у S_q корака.

Разрада Полиг-Хелмана

Подразумијевајући да смо нашли x_0, опет из $h = g^x$, закључујемо

$$h^{q^{e-2}} = g^{(x_0+x_1 q)q^{e-2}}.$$

Претходно се можемо трансформисати у

$$\left(g^{q^{e-1}}\right)^{x_1} = \left(g^{-x_0} h\right)^{q^{e-2}}.$$

Ово је, опет, ДЛОГ који можемо ријешити у S_q корака. Тиме смо нашли и x_1.

Разрада Полиг-Хелмана

- Настављајући претходно описани поступак, јасно је да редом можемо одредити све коефицијенте $x_0, x_1, \ldots, x_{e-1}$, а тиме и само рјешење x, оригиналног проблема $g^x = h$.
- Како је "цијена" сваког појединачног рјешавања ДЛОГ-а једнака S_q корака, онда је укупна цијена једнака eS_q.

Примјер Полиг-Хелмана

Нека је дат ДЛОГ

$$23^x = 9689 \pmod{11251}.$$

Број 23 је примитивни коријен у датом пољу, па је његов ред једнак 11250. Пошто је $11250 = 2 \cdot 3^2 \cdot 5^4$ производ степена малих простих бројева, онда је Полиг-Хелман ефикасан.

Примјер Полиг-Хелмана

q	e	$g^{(p-1)/q^e}$	$h^{(p-1)/q^e}$	$\left(g^{(p-1)/q^e}\right)^x = h^{(p-1)/q^e}$
2	1	11250	11250	1
3	2	5029	10724	4
5	4	5448	6909	511

Примјер Полиг-Хелмана

- До података у табели долазимо рачуном, као на примјер

$$g^{\frac{p-1}{2}} \equiv 11250 \pmod{11251},\ h^{\frac{p-1}{2}} \equiv 11250 \pmod{11251}.$$

- Слично, рјешавамо

$$\left(g^{\frac{p-1}{3^2}}\right)^x \equiv h^{\frac{p-1}{3^2}} \pmod{11251},$$

представљајући $x = c_0 + 3c_1$.

- На крају, из

$$x \equiv 1 \pmod{2},\ x \equiv 4 \pmod{3^2},\ x \equiv 511 \pmod{5^4},$$

добијамо $x = 4261$ као рјешење постављеног ДЛОГ-а.

Математичка припрема за RSA

Као што знамо, RSA је први асиметрични крипто-систем, настао седамдесетих година. Математичка основа RSA алгоритма је веома једноставна и дјелимично заснована на следећој теореми.

Теорема

Нека су p и q прости бројеви и нека је

$$g = (p-1, q-1).$$

Тада је

$$a^{\frac{(p-1)(q-1)}{g}} \equiv 1 \pmod{pq},$$

за свако a које задовољава $(a, pq) = 1$.

Математичка припрема за RSA

Као што знамо, Дифи-Хелман проблем и ЕлГамал почивају на тежини проблема рјешавања једначине $a^x \equiv b \pmod{p}$, гдје су a, b, p познате, а x непозната величина.
На другој страни, RSA почива на тежини проблема типа

$$x^e \equiv c \pmod{N},$$

гдје су e, c, N познате, а x непозната величина.

Теорема

Нека је p прост број, а $e \geq 1$ цио број за који вриједи $(e, p-1) = 1$. Тада конгруенција

$$x^e \equiv c \pmod{p}$$

има јединствено рјешење $x \equiv c^d \pmod{p}$ гдје је $de \equiv 1 \pmod{p-1}$.

Основна теорема RSA алгоритма

Следећа теорема представља срце RSA алгоритма и у директној вези је са претходном теоремом.

Теорема

Нека су p и q прости бројеви, а $e \geq 1$ цио број за који вриједи $(e, (p-1)(q-1)) = 1$. Тада конгруенција

$$x^e \equiv c \pmod{pq}$$

има јединствено рјешење $x \equiv c^d \pmod{pq}$ гдје је $de \equiv 1 \pmod{(p-1)(q-1)}$.

Хвала на пажњи :)