Gregor Leander
7.07.2008

Fakultät für Mathematik
Ruhr-Universität Bochum

Kryptographie II – Lösungsvorschläge zum Übungsblatt 5

Aufgabe 1 *Baby-Step-Giant-Step Algorithmus*
Berechnen Sie mit Hilfe des Baby-Step-Giant-Step Algorithmus den Diskreten Logarithmus von 67 zur Basis 5 in $\mathbb{Z}_{103}$.

Lösung
Wir berechnen zuerst $t = \lfloor\sqrt{102}\rfloor = 10$. Jetzt die beiden Tabellen. Zuerst die "Baby-Steps".

i	0	1	2	3	4	5	6	7	8	9	10
$5^i/67 \bmod 103$	20	100	88	28	37	82	101	93	53	59	89

Die "Giant-Steps":

j	0	1	2	3	4	5	6	7	8	9	10
$5^{-10j} \bmod 103$	1	28	63	13	55	98	66	97	38	34	25

Die gesuchte Kollision finden wir bei $i = 3$ und $j = 1$, d.h. es gilt

$$5^3/67 = 5^{-10} \bmod 103$$

und daher

$$67 = 5^{3+10} = 5^{13}.$$

Der gesuchte diskrete Logarithmus ist daher 13. □

Aufgabe 2 *Der Silver-Pohlig-Hellman Algorithmus*

1. Berechnen Sie mit Hilfe des Silver-Pohlig-Hellman Algorithmus den diskreten Logarithmus von 500 zur Basis 7 in $\mathbb{F}^*_{601}$.
2. Warum wird der Silver-Pohlig-Hellman Algorithmus praktisch unmöglich, wenn die Gruppenordnung durch eine Primzahl der Länge 60 Bit geteilt wird?
3. Wie kann man den Baby-Step-Giant-Step Algorithmus in Kombination mit dem Silver-Pohlig-Hellman Algorithmus nutzen, um Diskrete Logarithmen auch in der Situation von Aufgabenteil 2 zu berechnen?

4. Welche Anforderungen sollte man daher an die Gruppenordnung einer Gruppe G stellen, damit das Berechnen von Diskreten Logarithmen in G heutzutage praktisch unmöglich ist?

Lösung

1. Die Gruppe $\mathbb{F}_{601}^*$ mit der Multiplikation als Gruppenoperation ist zyklisch von der Ordnung
$$n = 600 = 2^3 * 3 * 5^2.$$
Wir wollen den diskreten Logarithmus x von $a = 500$ zur Basis $g = 7$ bestimmen (d.h. $7^x = 500$ in $\mathbb{F}_{601}$). Dazu bestimmen wir mit Hilfe des SPH Algorithmus zuerst
$$\begin{aligned} x_8 &= x \bmod 8 \\ x_3 &= x \bmod 3 \\ x_{25} &= x \bmod 25 \end{aligned}$$
und im zweiten Schritt x mit Hilfe des CRT.

   (a) **Bestimmen von** $x_8 = x \bmod 8$**:** Zuerst stellen wir eine Tabelle der Werte $r_{2,j} = 7^{300j}$ auf:

j	0	1
$r_{2,j}$	1	600

   Jetzt berechnen wir
$$a^{n/2} = a^{300} = 1 = r_{2,0}.$$
   Damit ist $j_0 = 0$ und wir setzen
$$a_1 = \frac{a}{g^0} = a.$$
   In der nächsten Iteration berechen wir
$$a_1^{n/4} = 600 = r_{2,1}$$
   und damit ist $j_1 = 1$. Wir setzen
$$a_2 = \frac{a_1}{g^{j0+2j_1}} = \frac{a_1}{g^2} = 47.$$
   Die letze Iteration liefert
$$a_2^{n/8} = 1 = r_{2,0}$$
   und somit $j_2 = 0$. Es gilt
$$x_8 = j_0 + 2j_1 + 4j_2 = 2.$$

(b) **Bestimmen von** $x_3 = x \bmod 3$**:** Zuerst stellen wir wieder die Tabelle der Werte $r_{3,j} = 7^{200j}$ auf:

j	0	1	2
$r_{3,j}$	1	576	24

Jetzt berechnen wir

$$a^{n/3} = a^{200} = 1 = r_{3,0}.$$

Damit ist $j_0 = 0$ und somit

$$x_3 = j_0 = 0.$$

(c) **Bestimmen von** $x_{25} = x \bmod 25$**:** Die Tabelle der Werte $r_{5,j} = 7^{120j}$ auf:

j	0	1	2	3	4
$r_{5,j}$	1	423	432	32	314

Jetzt analog zu oben

$$a^(n/5) = 314 = r_{5,4}$$

Damit ist $j_0 = 4$ und weiter $a_1 = 234$. Für j_1 berechnen wir

$$a1^(n/25) = 432 = r_{5,2}$$

und somit $j_1 = 2$. Es folgt

$$x_{25} = j_0 + 5j_1 = 4 + 10 = 14$$

Die gesuchte Lösung des Gleichungssystems

$$\begin{aligned} x &= 2 \bmod 8 \\ x &= 0 \bmod 3 \\ x &= 14 \bmod 25 \end{aligned}$$

ist (mittels CRT) $x = 114$. Dies kann man leicht durch die Probe

$$7^{114} = 500$$

bestätigen.

2. Hier wird es schwierig die Tabellen für die Werte $r_{p,j}$ aufzustellen. Dies kostet dann 2^{60} Operationen und genauso viel Speicherplatz.

3. Anstatt den diskreten Logarithmus mit Hilfe der Tabellen zu berechen, kann man auch den Baby-Step-Giant-Step Algorithmus nutzen. Der Aufwand (sowohl für Speicher also auch für Rechenzeit) ist dann nur $O(\sqrt{p})$ für einen Primteiler p der Gruppenordnung.

4. Wegen obigen Überlegungen sollte die Gruppenordnung einen Primteiler von 160 Bit Länge haben. Damit benötigt das Berechnen von diskreten Logarithmen mit dem SPH Algorithmus mindestens 2^{80} Operationen.

□

Aufgabe 3 *Index Calculus*
Bestimmen Sie mit dem Index Calculus Verfahren den Logarithmus von $X^3 + X^2 + 2$ in

$$\mathbb{F}_{3^5} = \mathbb{F}_3[X]/(X^5 - X + 1)$$

zur Basis X. Nutzen Sie als Faktorbasis

$$B = \{X, X + 1, X - 1\}$$

und als "Zufallszahlen" im ersten Schritt

$$t = \{20, 22, 23\}$$

und im zweiten Schritt

$$t = 19$$

Lösung
Es ist $f = X^5 - X + 1$ und

$$B = \{X, X + 1, X - 1\}$$

gegeben. Es soll der Logarithmus von

$$a = X^3 + X^2 + 2$$

zur Basis $g = X$ bestimmt werden. Zuerst bestimmt man die Logarithmen der Elemente in $\mathbb{F}_3^*$, d.h. von 1 und -1. Diese sind

$$\log_g(1) = 0 \text{ und } \log_g(-1) = 121.$$

Jetzt kommen die zwei Stufen des Index Calculus.

1. Im ersten Schritt sollen die Logarithmen der Faktorbasis bestimmt werden. Wir berechnen

$$\begin{aligned} g^{20} &= (X-1)^4 \bmod f \\ g^{22} &= -(X+1)^2(X-1) \bmod f \\ g^{23} &= -X(X+1)^2(X-1) \bmod f. \end{aligned}$$

   Daraus folgen die (linearen) Gleichungen

$$\begin{aligned} 20 &= 4\log_g(X-1) \\ 22 &= 121 + 2\log_g(X+1) + \log_g(X-1) \\ 23 &= 121 + 1 + 2\log_g(X+1) + \log_g(X-1) \end{aligned}$$

   und daraus $\log_g(X - 1) = 5$ und $\log_g(X + 1) = 69$.

2. Im zweiten Schritt berechnet man

$$ag^{19} = X^3 + 2X^2 = X^2(X-1)$$

und damit folgt

$$\log_g(a) + 19 = 2 + 5$$

und schließlich

$$\log_g(a) = 230 \bmod 242$$

□