Gregor Leander
7.07.2008

Fakultät für Mathematik
Ruhr-Universität Bochum

Kryptographie II – Lösungsvorschläge zum Übungsblatt 1

Aufgabe 1

Methode 1: Gegeben sind $(e, d) = (17, 412020005)$ und $n = 1000730021$. Daraus ergibt sich:

$$ed - 1 = 7004340084 = 2^2 \cdot 3 \cdot 7^2 \cdot 2381 \cdot 5003$$

Damit ergeben sich:

$$s = 2, \qquad u = 1751085021$$

Man kann nun $a = 2$ wählen und erhält dann im Schritt $j = 0$:

$$\begin{aligned} gcd((a^u)^{2^j} - 1, n) &= gcd((2^{1751085021})^{2^0} - 1, 1000730021) \\ &= gcd(418212544, 1000730021) \\ &= 10007 = p \end{aligned}$$

q ergibt sich dann zu $q = \frac{n}{p} = 100003$. Es funktioniert auch mit anderen a (und entsprechenden j). Die entsprechenden Maplebefehle:

```
A := 17;
B := 412020005;
C := 1000730021;
ifactor(A*B-1);
E := 2;
gcd(C,E);
S := 2;
U := ((A*B-1)/4);
F := E&^U mod C;
P := gcd((F)^(2^0)-1,C);
Q := C/P;
```

Die Variablen sind `A`= e, `B`= d, `C`= n und `E`= $\sigma(a)$ (Vgl. Algorithmus 8 im Skript).
Methode 2: Gegeben sind $(e, d) = (17, 412020005)$ und $n = 1000730021$. Daraus ergibt sich:

$$k = \left\lceil \frac{ed - 1}{n - 2\sqrt{n} + 1} \right\rceil = 7$$

Nun kann approximiert werden:

$$\sigma(k) = \frac{ed-1}{k} + n + 1 = 110010$$

Daraus ergibt sich die quadratische Gleichung $x^2 - \sigma(k)x + n = 0$ mit den Lösungen:

$$p, q = \begin{cases} 100003 \\ 10007 \end{cases}$$

Für diese Zahlen ergibt gleich das erste k die Lösung. Die entsprechenden Maplebefehle:

```
A := 17;
B := 412020005;
C := 1000730021;
E := isqrt(C);
K := K := trunc(evalf((A*B-1)/(C-2*E+1)))+1;
J := -((A*B-1)/7)+C+1;
solve({x^2-J*x+C},{x});
```

Die Variablen sind `A`= e, `B`= d, `C`= n und `J`= $\sigma(k)$.
Offensichtliche Schwäche: n hat die Form

$$1\{0\}^{viele}73\{0\}^{viele}21$$

wobei

$$7 \cdot 3 = 21$$

und

$$7 \cdot 10 + 3$$

gelten. Daher muss $p = 1\{0\}^x 7$ und $q = 1\{0\}^y 3$ gelten. Da der Mittelteil 73 anstatt von 37 ist, muss $y = x + 1$ gelten. Die Werte $x = 3$ und $y = 4$ ergeben sich dann durch Abzählen der Stellen. Diese Methode funktioniert für alle n der Form:

$$1\{0\}^{viele}(\sum)\{0\}^{viele}(\prod)$$

Man beachte, dass der Angreifer sich die günstigste Basisdarstellung aussuchen kann.

Aufgabe 1

A: Gesucht wird:

$$\begin{aligned} m &= \sqrt[3]{C} \\ &\equiv \left(c_1 N_1 (N_1^{-1} \bmod n_1) + c_2 N_2 (N_2^{-1} \bmod n_2) + c_3 N_3 (N_3^{-1} \bmod n_3)\right) \bmod n_1 n_2 n_3 \end{aligned}$$

Dabei gelten

$$\begin{aligned} N_1 &= n_2 n_3 &&= 34969 \\ N_2 &= n_1 n_3 &&= 80707 \\ N_3 &= n_1 n_2 &&= 192763 \end{aligned}$$

und:

$$\begin{aligned} (N_1^{-1} \bmod n_1) &= 110 \\ (N_2^{-1} \bmod n_2) &= 270 \\ (N_3^{-1} \bmod n_3) &= 109 \end{aligned}$$

Berechnung durchgeführt mit Maple, Konsolentext:

```
A := 289*121;
B := 667*121;
C := 667*289;
E := A^(-1) mod 667;
F := B^(-1) mod 289;
G := C^(-1) mod 121;
H := 667*121*289;
J := (167*A*E+60*B*F+56*C*G) mod H;
M := surd (J, 3);
```

Die Variablen sind `A`= N_1, `B`= N_2, `C`= N_3, `H`= $n_1 n_2 n_3$ und `J`= C.
B: Es muss

$$m^5 \overset{!}{<} \prod n_i$$

gelten, damit der Angriff für alle Nachrichten möglich ist. ($m < n_{min}$ wird vorrausgesetzt.)
Man erhält somit folgende Abschätzung:

$$\begin{aligned} (n_{min} - 1)^5 &\overset{!}{<} n_{min}^x \\ 5 \log(n_{min} - 1) &\leq x \log(n_{min}) \\ 5 &\leq x \end{aligned}$$

Man benötigt im Allgemeinen also mindestens 5 (teilerfremde) n_i.
