KRIPTOGRAFIJA
Zadaća 5.132

Filip Nikšić
fniksic@gmail.com

27. svibnja 2007.

1. Odaberite dva različita četveroznamenkasta prosta broja p i q. Neka je $n = p \cdot q$. Odaberite peteroznamenkasti broj e koji je relativno prost s $\varphi(n)$. Šifrirajte otvoreni tekst

$$x = 394694$$

pomoću RSA kriptosustava s javnim ključem (n, e). Odredite pripadni tajni ključ d.

Rješenje. Odaberimo proste brojeve

$$p = 5821, \qquad q = 6263\,.$$

Izračunamo:

$$n = p \cdot q = 36456923,$$
$$\varphi(n) = (p-1) \cdot (q-1) = 36444840.$$

Odaberimo sad $e = 2^{13} + 2^{11} + 1 = 10241$. Euklidovim algoritmom nalazimo da je

$$(e, \varphi(n)) = 886121 \cdot e - 249 \cdot \varphi(n) = 1\,,$$

prema tome, odabrani e je relativno prost s $\varphi(n)$. Osim toga, odmah nalazimo da je

$$886121 \cdot e \equiv 1 \pmod{\varphi(n)}$$

pa imamo $d = 886121$.

Ostaje šifrirati zadani otvoreni tekst, tj. izračunati $y = x^e \bmod n$. Vrijedi:

$$\begin{aligned} y &= x^e \\ &= x^{2^{13}+2^{11}+1} \\ &= x^{(2^2+1)\cdot 2^{11}} \cdot x \\ &= \left(x^{2^2} \cdot x\right)^{2^{11}} \cdot x \end{aligned}$$

Dakle, x moramo kvadrirati 2 puta, rezultat pomnožiti s x, novi rezultat kvadrirati 11 puta i na kraju još jednom pomnožiti s x. U svakom koraku rezultat reduciramo modulo n. Tablica međurezultata:

u (binarno)	$x^u \bmod n$	
1	394694	$t \leftarrow x$
10	2921657	$t \leftarrow t^2$
101	25655322	$t \leftarrow t^2 \cdot x$
1010	35209381	$t \leftarrow t^2$
10100	14998894	.
101000	8422525	.
1010000	25808381	.
10100000	25972709	.
101000000	26645106	.
1010000000	29189235	.
10100000000	24882945	.
101000000000	13442514	.
1010000000000	1176855	.
10100000000001	1077349	$t \leftarrow t^2 \cdot x$

Dobivamo $y = 1077349$. □

2. Alice je poslala istu poruku m nekolicini agenata. Eva je presrela šifrate c_1, c_2, c_3 za trojicu agenata čiji su javni ključevi n_1, n_2 i n_3. Poznato je da Alice i agenti koriste RSA sustav s javnim eksponentom $e = 3$.

Za zadane

$$\begin{aligned} n_1 &= 6557, & c_1 &= 5986, \\ n_2 &= 10573, & c_2 &= 3362, \\ n_3 &= 14351, & c_3 &= 12352, \end{aligned}$$

pomozite Evi da otkrije poruku m.

Rješenje. Označimo $y = m^3$. Iz zadatka doznajemo da je

$$\begin{aligned} y &\equiv c_1 \pmod{n_1}, \\ y &\equiv c_2 \pmod{n_2}, \\ y &\equiv c_3 \pmod{n_3}. \end{aligned}$$

Prema kineskom teoremu o ostatcima, moramo riješiti tri linearne kongruencije:

$$\begin{aligned} n_2 n_3 y_1 &\equiv c_1 \pmod{n_1}, \\ n_1 n_3 y_2 &\equiv c_2 \pmod{n_2}, \\ n_1 n_2 y_3 &\equiv c_3 \pmod{n_3}. \end{aligned}$$

Rješavamo ih Euklidovim algoritmom. Naime, dobijemo:

$$\begin{aligned} (n_2 n_3, n_1) &= -1589 \cdot n_2 n_3 + 36770464 \cdot n_1 = 1 &\implies& y_1 = -1589 \cdot c_1 \bmod n_1 = 2453, \\ (n_1 n_3, n_2) &= -1260 \cdot n_1 n_3 + 11213977 \cdot n_2 = 1 &\implies& y_2 = -1260 \cdot c_2 \bmod n_2 = 3653, \\ (n_1 n_2, n_3) &= 5188 \cdot n_1 n_2 - 25062317 \cdot n_3 = 1 &\implies& y_3 = 5188 \cdot c_3 \bmod n_3 = 4961. \end{aligned}$$

Kineski teorem o ostatcima sad kaže da je rješenje dano s

$$\begin{aligned} &y \equiv n_2 n_3 y_1 + n_1 n_3 y_2 + n_1 n_2 y_3 \pmod{n_1 n_2 n_3}, \text{ tj.} \\ &y = 64964808000. \end{aligned}$$

Dakle, $m = \sqrt[3]{64964808000} = 4020$. □

3. Neka je (e, n) Bobov javni RSA ključ. Poznato je da tajni eksponent d zadovoljava nejednakost $d < \frac{\sqrt[4]{n}}{3}$. Odredite d (Bobov tajni ključ) i pomoću njega dešifrirajte poruku c koju je Alice poslala Bobu.

Ulazni podatci su

$$
\begin{aligned}
e &= 10038737176255, \\
n &= 128444377819369, \\
c &= 81771654228766.
\end{aligned}
$$

Rješenje. Prema Wienerovom teoremu, d je dovoljno tražiti među nazivnicima konvergenata u razvoju u verižni razlomak broja e/n. Kako razviti e/n u verižni razlomak? Znamo da možemo pisati $e = n \cdot a_0 + r_0$, gdje je $a_0 = \lfloor e/n \rfloor$, $0 \leqslant r_0 < n$. No tada je

$$
\frac{e}{n} = a_0 + \frac{r_0}{n} = a_0 + \frac{1}{\frac{n}{r_0}}\,.
$$

Nadalje, imamo $n = r_0 \cdot a_1 + r_1$, gdje je $a_1 = \lfloor n/r_0 \rfloor$, $0 \leqslant r_1 < r_0$. Slijedi:

$$
\frac{e}{n} = a_0 + \frac{1}{a_1 + \frac{r_1}{r_0}} = a_0 + \frac{1}{a_1 + \frac{1}{\frac{r_0}{r_1}}}\,.
$$

Tako nastavljamo dalje. Pretpostavimo da smo pronašli i provjerili sve konvergente do $p_{i-1}/q_{i-1} = [a_0, \ldots, a_{i-1}]$:

1. Izračunamo $a_i = \lfloor r_{i-2}/r_{i-1} \rfloor$ i $r_i = r_{i-2} - r_{i-1}a_i$.
2. Izračunamo q_i iz rekurzije $q_i = a_i q_{i-1} + q_{i-2}$ uz početne uvjete $q_0 = 1$, $q_1 = a_1$.
3. Modularnim potenciranjem (kao u zadatku 1) provjerimo vrijedi li $(x^e)^{q_i} \equiv x \pmod{n}$ za npr. $x = 2$. Ukoliko vrijedi, $d := q_i$, inače tražimo sljedeću konvergentu.

U svrhu provjere u 3. koraku izračunajmo odmah 2^e mod n modularnim potenciranjem: 2^e mod $n = 64951227442387$. Naravno, zbog uvjeta zadatka, d će se pojaviti prije nego q_i prijeđe $\sqrt[4]{n}/3 \approx 1122$. Međurezultate možemo pregledno prikazati u tablici:

i	a_i	r_i	q_i	$(2^e)^{q_i}$ mod n
0	0	10038737176255	1	64951227442387
1	12	7979531704309	12	15952718268460
2	1	2059205471946	13	14440921883618
3	3	1801915288471	51	115413908793396
4	1	257290183475	64	62592196965771
5	7	884004146	499 ✓	2

Dakle, tajni eksponent $d = 499$. Ostaje dešifrirati tajnu poruku c, tj. izračunati c^d mod n. Ovo opet radimo modularnim potenciranjem. Rezultat:

$$
c^d \bmod n = 13937633503473\,.
$$

□