RUHR UNIVERSITÄT BOCHUM

RUB

Lehrstuhl für Kryptologie und IT-Sicherheit
Prof. Dr. Alexander May
Ilya Ozerov, Elena Kirshanova

Hausübungen zur Vorlesung

Kryptanalyse

SS 2014

Blatt 8 / 30 June, 2014

Exercise 1 (5 Punkte)**:**
Consider DSA signature scheme. Let (p, q, α, β) be a public key and a a secret key with q being a big prime divisor of p and $\beta = \alpha^a \bmod p$. To sign a message $m \in \mathbb{Z}_q^*$, one computes a pair

$$\text{sig}(m) = (\gamma, \delta) = (\alpha^r \bmod p \bmod q, r^{-1}(m + a\gamma) \bmod q)$$

for random $r \in \mathbb{Z}_q^*$.
Show how to compute the secret key a

1. if the randomness r is known (and $\gamma \neq 0$);
2. if you are given two signatures $\text{sig}(m)$, $\text{sig}(m')$, $m \neq m'$ generated under the same key and the same randomness r. *Hint:* reduce the problem to finding the randomness r.

Now we analyze the situation where a sender signs n messages m_i using his fixed private key and different randomness r_i. But due to a bad random generator all r_i's happened to be 'small', i.e. $r_i < X_i, i = 1 \dots n$. In other words, we have the following set of congruences

$$m_i + a\alpha^{r_i} - r_i\delta_i = 0 \bmod q.$$

1. Transform the above set of equations to the form

   $$y_i + y_0 A_i + B_i = 0 \bmod q \quad i = 1 \dots n,$$

   for some known A_i, B_i and unknown y_i.
2. In order to find a small solution to the set of above congruences, construct an $(n+1)$-dimensional lattice L, s.t. the solution vector $\mathbf{y} = (y_0, y_1, \dots, y_n)$ solves the CVP instance on L for the target vector $\mathbf{t} = (0, B_1, \dots, B_n)$.
3. There is a polynomial time algorithm called the Babai's algorithm that finds a close lattice-point $\mathbf{v}$ to a given non-lattice point $\mathbf{t}$ in an $(n+1)$-dimensional lattice, s.t.

   $$\|\mathbf{v} - \mathbf{t}\| \leq c_1 \|\mathbf{b}_{n+1}^*\|,$$

   for some constant c_1. Use the following heuristic estimation for $\|\mathbf{b}_{n+1}^*\|$:

   $$\|\mathbf{b}_{n+1}^*\| \leq c_2 (\det L)^{\frac{1}{n+1}},$$

   for some another constant c_2, to provide an upper-bound on X_i's such that the Babai's algorithm will output the randomness used in the signatures.

Exercise 2 (4 Punkte)**:**
Let $N = pqr$, $p > q > r$. Assume you are given $\tilde{p}$ – an approximation for p with

$$|p - \tilde{p}| \leq N^{\frac{1}{9}}.$$

Show how to factor N in time polynomial in $\log N$.

Exercise 3 (10 Punkte)**:**
To solve this problem you can use any computer algebra system you like. You are given an RSA-modulus $N = pq$ and a good approximation $\tilde{p}$ to p:

$N =$ 11 700 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000
000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000
000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000
000 008 489 000 000 000 000 000 000 000 305 100 000 000 000 000 000 000 000 000 000 000
000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000
000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000
000 000 000 000 000 000 000 000 000 000 221 367

$\tilde{p} =$ 12 999 999 999 999 999 999 999 999 999 999 999 999 999 999 999 999 999 999 999
999 999 999 999 999 999 999 999 999 999 999 999 999 999 999 999 999 999 999 999 998 976
578 640 663 186 879 694 547 858 288 860 261 055 699 575 395 225 989 520 569 851 572 568
902 279 408 524 976 606 706 603 183 191 359 488

Factor N.