Cryptography (SS2006) Prof. Michael Backes

Solutions for Exercise Sheet 8

Out: 06/28/2006 Saarland University

Problem 1: Wiener's Attack

We know that $N = 99221$ and $e = 39437$ and that $d \leq \frac{1}{3}N^{0.25}$. We compute the continued fraction expansion of $\frac{e}{N}$ using the Euclidean Algorithm:

$$\begin{aligned}
39437 &= 0 \cdot 99221 + 39437 \\
99221 &= 2 \cdot 39437 + 20347 \\
39437 &= 1 \cdot 20347 + 19090 \\
20347 &= 1 \cdot 19090 + 1257 \\
19090 &= 15 \cdot 1257 + 235 \\
1257 &= 5 \cdot 235 + 82 \\
235 &= 2 \cdot 82 + 71 \\
82 &= 1 \cdot 71 + 11 \\
71 &= 6 \cdot 11 + 5 \\
6 &= 1 \cdot 5 + 1 \\
5 &= 5 \cdot 1 + 0
\end{aligned}$$

Thus, the continued fraction expansion of $\frac{39437}{99221}$ is $[0, 2, 1, 1, 15, 5, 2, 1, 6, 1, 5]$

The convergents are:

$0, \frac{1}{2}, \frac{1}{3}, \frac{2}{5}, \frac{31}{78}, \frac{157}{395}, \frac{345}{868}, \frac{502}{1263}, \frac{3357}{8446}, \frac{7216}{18155}, \frac{39437}{99221}$

Compute candidates for $M = \varphi(N)$ using $e \cdot d - k \cdot \varphi(N) = 1$.

$$\begin{aligned}
M_1 &= \frac{39437 \cdot 2 - 1}{1} = 78873 \\
M_2 &= \frac{39437 \cdot 3 - 1}{1} = 118310 \\
M_3 &= \frac{39437 \cdot 5 - 1}{2} = 98592 \\
&\vdots
\end{aligned}$$

We have $N = p \cdot q$ and $\varphi(N) = (p-1) \cdot (q-1)$

$\Rightarrow p_{1,2} = \frac{N-\varphi(N)+1}{2} \pm \sqrt{\left(\frac{N-\varphi(N)+1}{2}\right)^2 - N}$

For M_3 we get $p = 313$ and because of $N = p \cdot q$ also $q = 317$. And of course $313 \cdot 317 = 99221$.

Problem 2: Breaking ElGamal Signatures

(a) Given r, m and $sig = (s, t)$. We assume that s is invertible modulo $p - 1$, which is true with high probability, as $p - 1$ should have a large prime factor.

We know by construction that

$$\begin{aligned} t &= (m - xs) \cdot r^{-1} \bmod p - 1 \\ r \cdot t &= m - xs \bmod p - 1 \\ x &= (m - rt) \cdot s^{-1} \bmod p - 1 \end{aligned}$$

(b) Provided that the same random value r is used in both signatures $sig_1 = (s_1, t_1)$ and $sig_2 = (s_2, t_2)$, they have the form

$$\begin{aligned} s &:= s_1 = s_2 = g^r \bmod p, \\ t_1 &= (m_1 - xs)r^{-1} \bmod p - 1 \\ t_2 &= (m_2 - xs)r^{-1} \bmod p - 1 \end{aligned}$$

This implies that

$$\begin{aligned} r &= (m_1 - xs)t_1^{-1} \bmod p - 1 \\ &= (m_2 - xs)t_2^{-1} \bmod p - 1 \end{aligned}$$

and consequently

$$(m_1 - xs)t_2 = (m_2 - xs)t_1 \bmod p - 1$$

and

$$x = (t_1 m_2 - t_2 m_1)s^{-1}(t_1 - t_2)^{-1} \bmod p - 1$$

Again we need that certain elements are invertible, but again this does not decrease our success probability substantially.

Problem 3: Breaking DSA Signatures

We are given a "DSA signature" (s, t) for a message m where $t = 0$. This implies

$$t = 0 = (\mathsf{H}(m) + xs)r^{-1} \bmod q.$$

As there are no zero divisors modulo q, as q is a prime, we have

$$\mathsf{H}(m) + xs = 0 \bmod q,$$

and consequently we can compute

$$x := -\mathsf{H}(m) \cdot s^{-1} \bmod q.$$