RUHR UNIVERSITÄT BOCHUM

RUB

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

Hausübungen zur Vorlesung

Kryptanalyse I

SS 2015

Blatt 1 / 16. April 2015

Abgabe bis: 30. April 12:00 Uhr, Kasten NA/02

Aufgabe 1 (3 Punkte)**:**
Show that RSA with N being prime is insecure.

Aufgabe 2 (3 Punkte)**:**
Let $N = pq$, for two distinct primes p and q, and let $\gcd(e, \phi(n)) = 1$. Show that

$$\begin{aligned} \mathrm{RSA}_e : \mathbb{Z}_N^* &\to \mathbb{Z}_N^* \\ x &\to x^e \end{aligned}$$

is bijective.

Aufgabe 3 (5 Punkte)**:**
Hastad's Broadcast Attack. Imagine a secret announcement letter M has been sent to three parties. Each party has its public key pair (N_i, e_i) for $i = 1, \ldots 3$, where $e_i = 3$ for all i (we assume here that $\gcd(N_i, N_j) = 1, j \neq i$). Eve wants to know the content of the secret letter. All she sees, however, are three ciphertexts

$$c_1 = M^3 \bmod N_1 \qquad c_2 = M^3 \bmod N_2 \qquad c_3 = M^3 \bmod N_3$$

Assuming that $M < N_i$ for all i, help Eve to recover M.

Aufgabe 4 (10 Punkte)**:**
Programming assignment. You are given an oracle-access to a function `dec(c)` that inverts the $\mathrm{RSA}_{N,d}$ function: on input c it computes $m = c^d \bmod N$ for all but one ciphertext. We call this ciphertext a challenge-ciphertext c^*. The parameters (N, e, d, c^*) are fixed. You'll find all public parameters in the file 'params.txt'. Your task is to decrypt the challenge c^*. To accomplish the task you should follow the instruction below (**Important!** You will need to have the GMP library installed on your machine (`www.gmplib.org`):

Instructions (for Linux):

1. Download the two files 'dec.o' and 'dec.h' from the web-page.

   It provides the function

   ```
   char* dec (const char *c_inp)
   ```

   that returns the decryption of a ciphertext `c_inp` given as a string for fixed (N, d). You can also provide a ciphertext of the GMP long int type by calling

```
char* dec (mpz_t *c_inp)
```

2. To use the above function, either create your own .cpp file and include 'dec.h' as a header or download the template file 'hw1.cpp' from the web-site. To compile this .cpp file with the 'dec.o' run in terminal

   ```
   g++ hw1.cpp dec.o -lgmp
   ```

   Don't forget to link it with the GMP library!

3. As the result, you should get a .out file which you can then execute.

As this is an attack on a public key cryptosystem and you are given e, you should implement the corresponding encryption function by yourself. You should submit both the resulting $\mathtt{m} = \mathtt{dec}(\mathtt{c}^*)$ and your code.

Instructions (for Windows):

1. Find a machine with Linux.

2. Follow the instructions above.