The electronic health card, summer 2008

MICHAEL NÜSKEN, DANIEL LOEBENBERGER

4. Exercise sheet
Hand in solutions until Monday, 19 May 2008.

Exercise 4.1 (RSA). (7+1 points)

Using the primes $p = 31$ and $q = 41$ an RSA system shall be set up. (In practice these primes are of course much too small!) We choose $e = 17$ and $N = p \cdot q$ as public key.

(i) Use the extended Euclidean algorithm to compute the corresponding secret key d such that $e \cdot d \equiv 1 \bmod \varphi(N)$. *Important:* Write down all steps in the extended Euclidean algorithm! [3]

(ii) Encrypt $x = 1\,190$. [2]

(iii) Decrypt $y = 1\,026$. [2]

If you use a computer algebra system, as for example MuPAD or MAPLE then hand in (a printout of) your program sources and outputs (including intermediate results of the extended Euclidean algorithm), and use the following values instead: [+1]

$$\begin{aligned} p &= 2\,609\,899, \\ q &= 3\,004\,217, \\ e &= 54\,323\,425\,121, \\ x &= 4\,364\,863\,612\,562, \\ y &= 850\,080\,551\,629. \end{aligned}$$

Exercise 4.2 (Cracking RSA). (9 points)

Write a program for the following:

(i) Generate random RSA keys with N about 200 Bits. Keep the private key (N, d) secret and tell only the public key. Do not throw away anything this time. [You may assume that MuPAD's `random(`a`..`b`)` yields a function(!) outputting *uniformly random* numbers in the interval $a..b$.] [2]

(ii) Use only N and L to recover the primes. [3]

[4] (iii) Compute a second pair (e', d') and use the two pairs (and possibly N) to recover L.

Exercise 4.3 (ElGamal signatures). (7 points)

Compute an ElGamal signature for your student identification number represented in binary. Use $p = 467$ and $g = 3 \in \mathbb{Z}_p^\times$ and work in $G = \langle g \rangle$. For simplicity, we take the function HASH: $\{0,1\}^* \to \mathbb{Z}_{233},\ x \mapsto (\sum_{0 \le i < |x|} x_i 2^i) \bmod 233$. (Eg. 18 translates to the string 10010 which in turn translates into the number $18 \bmod 233$.)

[1] (i) Here $\#G = 233$ and thus $\exp_g \colon \mathbb{Z}_{233} \to G,\ a \mapsto g^a$ is an isomorphism. [Note that $166^2 = 3$ and thus $g^{233} = 1$. Since $g \neq 1 \ldots$]

[1] (ii) Setup: Compute Alice' public key with $\alpha = 9$.

[3] (iii) Sign: Sign the hash value of your student identification number.

[2] (iv) Verify: Verify the signature.

Exercise 4.4 (RSA Hardcore Bit). (6+6 points)

In this exercise we will examine the question whether an algorithm that gives you partial information on the plaintext (given the public key and the ciphertext) already gives you the complete plaintext.

[6] (i) First assume that you are given an algorithm $\mathcal{A}$ that on input (N, e, y) outputs the least significant bit of the plaintext x (so it says whether x is even or odd). Construct given $\mathcal{A}$ an algorithm $\mathcal{B}$ that will give you on input (N, e, y) the whole plaintext x. [Hint: If $\mathcal{A}(N, e, y) = 0$ then $x = 2x'$. Otherwise note that N is odd!]

[+3] (ii) Often one has probabilistic algorithms which will not always give the correct answer, but work with a certain error probability. You are now going to explore how such an algorithm would behave in our setting. So assume now that the algorithm $\mathcal{A}$ has a small error probability of 2^{-n} where n is the number of bits in N. Compute the probability that your algorithm $\mathcal{B}$ returns the correct plaintext. [Hint: The Bernoulli inequality states that $(1 + x)^r \ge 1 + rx$ for $x > -1$ and $r \ge 0$.]

[+3] (iii) Finally assume that the atticking algorithm has a huge error probability of 40%. Can you still compute the entire plaintext efficiently?

Exercise 4.5 (Encryption and decryption with AES). (0+6 points)

(i) Given the output of the function ByteSub, how can you find the corresponding input? +1

(ii) Compute the inverse of $t_1 = x^4 + x^3 + x^2 + x + 1 \in \mathbb{F}_{256}$. +1

(iii) Compute the inverse of $t_2 = z^4 + z^3 + z^2 + z + 1 \in \mathbb{F}_2[z]/\langle z^8 + 1\rangle$. +1

(iv) Verify that the product of the polynomial $d = \texttt{0B}y^3 + \texttt{0D}y^2 + \texttt{09}y + \texttt{0E}$ and the polynomial $c = \texttt{03}y^3 + \texttt{01}y^2 + \texttt{01}y + \texttt{02}$ is equal to $\texttt{1}$ in the ring $\mathbb{F}_{256}[y]/\langle y^4 + 1\rangle$. +3