Cryptography, winter term 16/17: Sample solution to assignment 9

Cornelius Brand, Marc Roth

Exercise 9.1 (Be nice to your tutors and TAs, 1 Bonus Point) Write the name and matriculation number of every author as well as number, time slot and the name of the tutor of your tutorial group on the first page of your solution. Furthermore write in english and staple *all* sheets of your solution.

Exercise 9.2 (RSA and Factoring, 2+1+2+3 Points) The following exercises can and should be solved without using an electronic calculator.

(a) Calculate $\gcd(352, 17)$ via the extended euclidian algorithm and compute s and t such that $\gcd(352, 17) = s \cdot 352 + t \cdot 17$.

(b) Compute $d := 17^{-1} \bmod \Phi(391)$. **Hint:** 23 is a divisor of 391.

(c) Compute x such that $x^{17} = 49 \bmod 391$. You may use that $49^{29} = 2 \bmod 391$.

(d) Prove that hardness of *RSA-Inv* implies hardness of *Factoring*, i.e., assume the existence of a ppt adversary $\mathcal{A}$ that wins the Factoring-Experiment with non-negligible probability and use it to construct a ppt adversary that wins the RSA-Inv experiment with non-negligible probability.

Solution 9.2 (RSA and Factoring, 2+1+2+3 Points)

(a) Applying the extended euclidian algorithm yields:

$$\begin{aligned} 352 &= 20 \cdot 17 + 12 \\ 17 &= 1 \cdot 12 + 5 \\ 12 &= 2 \cdot 5 + 2 \\ 5 &= 2 \cdot 2 + 1 \end{aligned}$$

It follows that $\gcd(352, 17) = 1$. We continue as follows:

$$\begin{aligned} 1 &= 5 - 2 \cdot 2 \\ &= 5 \cdot 5 - 2 \cdot 12 \\ &= 5 \cdot 17 - 7 \cdot 12 \\ &= 145 \cdot 17 - 7 \cdot 352 \end{aligned}$$

(b) Using the hint, we get that $391 = 23 \cdot 17$. As 23 and 17 are primes it holds that $\Phi(391) = 22 \cdot 16 = 352$. Using (a) we conclude that $145 = 17^{-1} \bmod 352$.

(c) From (b) we know that $145 = 17^{-1} \bmod 352$ and hence it follows that $x := 49^{145}$ satisfies the equation. (The argument is explained in the solution of (d)). Now we have

$$49^{145} = (49^{29})^5 = 2^5 = 32 \bmod 391\,.$$

(d) We construct an adversary $\mathcal{A}'$ that wins the RSA-Inv experiment with non-negligible probability as follows. Upon being given (N, e, y), we first simulate the assumed adversary $\mathcal{A}$ on N to obtain (p, q). If $p \cdot q \neq N$, output a random guess for x. If $N = p \cdot q$, compute $\phi(N) = (p-1)(q-1)$. Using the extended euclidean algorithm, compute $d = e^{-1}$ modulo $\phi(N)$, and output $x := y^d$. Clearly, the algorithm is ppt, and since $\mathcal{A}$ wins with non-negligible probability, the case that $\mathcal{A}'$ in fact receives a factorization of N from $\mathcal{A}$ appears with non-negligible probability. If this is the case, then by construction, $x^e = (y^d)^e = (y^{e^{-1}})^e = y$ modulo N. Thus, the probability of $\mathcal{A}'$ winning the RSA-Inv experiment is at least that of $\mathcal{A}$ winning the factoring experiment, which was non-negligible by assumption.

Exercise 9.3 (Miller-Rabin-Test, 4 Points + 2 Bonus Points) The proof of correctness of the Miller-Rabin primality test you saw in the lecture left two gaps open, which we will address in this exercise. As usual, inputs will be coded in binary, so to represent a natural number t you need at most $\log t + 1$ bits. This is important: You will have to show that your algorithms run in polynomial time in the *size* of the numbers given as input (and not in the absolute value of the input numbers, which might be exponentially larger than the number of bits needed to represent it). You may assume without proof that arithmetic operations on numbers can be performed in polynomial time in their size. Keep in mind that you still have to argue that the resulting numbers stay of polynomial size in the size of n (e.g., 2^{2^n} is not computable in polynomial time).

(a) Show how to decide whether a given natural number $n > 1$ is a perfect power[1] in polynomial time.
Hint: Try to bound the maximal value of the exponent b polynomially in the size of n. You can then go through all exponents iteratively, and in each step decide in polynomial time in the size of n whether there is a basis a for the current exponent b, using a suitable search algorithm.

(b) **Bonus:** Given a natural number $n \in \mathbb{N}$ and $a \in \mathbb{Z}_n^*$, show how to decompose $n - 1 = 2^r u$ with u odd and $r \geq 1$ in polynomial time (argue why $r \geq 1$ when executing the Miller-Rabin test!) Then, show how to decide whether a is a strong witness that n is composite in polynomial time.
Hint: Review the exercises from last week's presence exercise sheet. Do you see one that seems related?

Do not forget to prove correctness and any claimed bound on the running time of your algorithms!

[1] Recall that a natural number $n \in \mathbb{N}$ is called a *perfect power* if there are $a, b \in \mathbb{N}$ such that $a^b = n$ and $a, b > 1$.

Solution 9.3 (Miller-Rabin-Test, 4 Points + 2 Bonus Points) (a) Let $||n|| \leq \log n + 1$ be the size of the input n. Clearly, for all natural numbers $a > 1$, $a^{||n||} \geq n$. This limits the range of search for the exponent b to $b \in B := \{1, \ldots, ||n||\}$. Conversely, for any fixed $b > 1$, the range of possible values of a is limited to the set $A := \{1, \ldots, n\}$. The algorithm proceeds as follows: For $\hat{b} = 1, \ldots, ||n||$, perform a binary search for the value n on the set of key-value pairs $\{(1, 1^{\hat{b}}), (2, 2^{\hat{b}}), \ldots, (n, n^{\hat{b}})\}$. If the binary search finds a pair (k, v) with $v = n$, output `YES`. If, on the other hand, all binary searches for all values of $\hat{b}$ find no such element, output `NO`.

Correctness follows from monotonicity of $x \mapsto x^b$ for all fixed b and the bound on b given before.

As for the running time: By the bound on $||n||$, there are a number of iterations linear in $\log n$, and each iteration uses an amount of time also polynomial in $\log n$, by the complexity of binary search and arithmetic operations (note that the sizes of all occurring numbers are bounded polynomially in n). In total, the procedure takes time polynomial in $\log n$, which is polynomial in the input size.

(b) If $r = 0$, then $n - 1$ odd, and n is even, which is excluded beforehand by the Miller-Rabin test. Regardless of this, the exponent r is then number of trailing zeroes in the binary expansion of $n-1$, and u the prefix up to this trailing sequence of zeroes. Reading this off clearly takes polynomial time in the size of $n - 1$ and hence n. Equivalently, the decomposition $n - 1 = 2^r \cdot u$ can be found in polynomial time by repeatedly halving $n - 1$ until the result of this operation is odd. The number of iterations this took is r, the remaining number is u.This works in polynomial time since $r \leq \log n$, and r decreases in each step.

Now, once r and u were found, we can square a^u repeatedly modulo n, and record the resulting sequence $(a^u, a^{2u}, \ldots, a^{2^r u})$ of length r. This uses a polynomial (in the size of n) number of operations to compute each square from the previous one, and since the size of the numbers (we are modulo n) are bounded by the size of n, we don't have to worry about too large numbers resulting. It is then a trivial matter to decide whether a is a strong witness for n being composite, by checking if it is of the form $(\ldots, -1, 1, \ldots, 1)$, where any ellipsis $\ldots$ may be an empty sequence.

Exercise 9.4 (RSA and Hash functions, 1+2+1 Points) Consider the following hash function (Gen, H):

- Gen: On input 1^n we run $\mathrm{GenRSA}(1^n)$ to get N, e and d. We choose $y \in \mathbb{Z}_N^* \setminus \{1\}$ uniformly at random and output $s = (N, e, y)$.
- H: Given a key $s = (N, e, y)$ and an input $x \in \{0,1\}^{3n}$, H^s is defined as

$$H^s(x) := f^s_{x_{3n}}(f^s_{x_{3n-1}}(\ldots f^s_{x_1}(1)\ldots))$$

where $f^s_0, f^s_1 : \mathbb{Z}_N^* \to \mathbb{Z}_N^*$ such that

$$f^s_0(a) := [a^e \bmod N] \text{ and } f^s_1(a) := [a^e \cdot y \bmod N]\,.$$

Note that the image of f_1^s, f_0^s is $\mathbb{Z}_N^*$ as this group is closed under multiplication (modulo N).

In this exercise you are asked to prove that hardness of *RSA-Inv* (relative to GenRSA) implies that (Gen, H) is collision-resistant. It may be advisable to proceed as follows

a) Show that f_0^s and f_1^s are bijections for fixed s.

b) Now assume a collision $a \neq b$ was found, i.e. $H^s(a) = H^s(b)$. Define

$$a^0 = 1 \text{ and } a^{i+1} = f^s_{a_{i+1}}(a^i)$$

and

$$b^0 = 1 \text{ and } b^{i+1} = f^s_{b_{i+1}}(b^i)\,.$$

Prove that there is an index j such that (i) $a^j \neq b^j$, (ii) $a^{j+1} = b^{j+1}$, and (iii) $a_{j+1} \neq b_{j+1}$.

c) Conclude that there are distinct u and v such that $f_0^s(u) = f_1^s(v)$ and show how to construct x from u and v such that

$$x^e = y \bmod N\,.$$

Example: Assume $s = (1111, 0111, 0100)$, i.e. $N = 15, e = 7$ and $y = 4$. Furthermore, let $x = 011100110001$. Then

$$H^s(x) = f_1^s(f_0^s(f_0^s(f_0^s(f_1^s(f_1^s(f_0^s(f_0^s(f_1^s(f_1^s(f_1^s(f_0^s(1)))))))))))$$

where

$$f_0^s(a) := [a^7 \bmod 15] \text{ and } f_1^s(a) := [a^7 \cdot 4 \bmod 15]\,.$$

Solution 9.4 (RSA and Hash functions, 1+2+1 Points) In the following we fix $s = (N, e, y)$ and write d^{-1} for the inverse of d in the group $\mathbb{Z}_N^*$, d^{-e} for the e-th root of d modulo N [2] and f_0, f_1 for f_0^s, f_1^s, respectively.

(a) We first show that f_0 and f_1 are surjective: For $c \in \mathbb{Z}_N^*$ it holds that $f_0(c^{-e}) = c$ and $f_1((y^{-1}c)^{-e}) = c$. Now bijectivity follows from surjectivity and the fact that domain and image are finite and of equal size.

(b) As $a \neq b$ there has to be a minimal index $i > 0$ such that $a_i \neq b_i$. As i is minimal it holds that $a^{i-1} = b^{i-1}$ and therefore

$$a^i = f_{a_i}(a^{i-1}) \neq f_{b_i}(a^{i-1}) = f_{b_i}(b^{i-1}) = b^i$$

where the inequality follows from the fact that $y \neq 1$ and $a_i \neq b_i$. Now as $H(a) = H(b)$ we have that $a^{3n} = b^{3n}$. Therefore, there exists j satisfying (i) and (ii) such that $i \leq j < 3n$. We claim that (iii) is also satisfied. Assuming not, it follows that $f_{a_{j+1}}(a^j) = f_{a_{j+1}}(b^j)$ which contradicts the fact that f_0 and f_1 are bijective. Hence, (iii) holds.

[2] Note that the e-th root exists for all $d \in \mathbb{Z}_N^*$, since $\gcd(e, \Phi(N)) = 1$.

(c) Let j be as in (b) and assume WLOG that $a_{j+1} = 0$ and $b_{j+1} = 1$. Furthermore, let $u := a^j$ and $v := b^j$. Then it holds that $f_0(u) = f_1(v)$, i.e.

$$u^e = v^e \cdot y \bmod N\,.$$

As $\mathbb{Z}_N^*$ is an abelian group, we conclude that

$$(u \cdot v^{-1})^e = y \bmod N\,.$$

Finally, this induces a reduction for the case $y \neq 1$. If $y = 1$, the e-th root of y can easily be computed.