# Cryptography, winter 2014/2015

PRIV.-DOZ. DR. ADRIAN SPALKA, DR. DANIEL LOEBENBERGER

## 10. Exercise sheet
## Hand in solutions until
## Wednesday, 21 January 2015, 23:59:59

**Exercise 10.1** (NIST test suite). (7 points)

In the lecture we played with the NIST statistical test suite from

`http://csrc.nist.gov/groups/ST/toolkit/rng/index.html`

(i) Download the test suite and make it run on your computer. [1]

(ii) Explain in your own words what the suite is doing. You might want to consult the documentation for this task. [3]

(iii) In the lecture we analyzed the results of a generator whose output can be found in the file `data/data.bad_rng`. Assess the file and explain the outcome of the test results. Hint: Ask yourself what "bad" means for a statistical test for cryptographic random number generators. [3]

**Exercise 10.2** (ElGamal Encryption). (7 points)

For a finite group $G$, recall that for $a \in G$ holds: $a$ is an element of order $d$ in $G$ if and only if $a^d = 1$ and $a^{d/t} \neq 1$ for all prime divisors $t > 1$ of $d$.

Let $p = 146\,347$. We implement the ElGamal encryption scheme using the group $\mathbb{Z}_p^\times$. As in the lecture we encode letters as follows: `A` is mapped to $0$, `B` to $1$ and so forth, `Z` is mapped to $25$. We combine groups of three letters $(a_0, a_1, a_2)$ to $a_0 + 26a_1 + 26^2a_2$. Thus `ABC` corresponds to the value $0 + 26 \cdot 1 + 2 \cdot 26^2 = 1378$.

(i) Check if $p$ is prime. Using (i) show that $23$ has order $24391$ in $\mathbb{Z}_{146347}^\times$. Note that $146346 = 2 \cdot 3 \cdot 24391$. [1]

(ii) Encrypt the word "`SYSTEM`" using the ElGamal scheme with $G = \langle g \rangle = \{1, g, g^2, \ldots\} \subseteq \mathbb{Z}_p^\times$, where $g = 23$. The receiver of the message has published the public key $A \leftarrow g^a = 76441$. Choose your public key to be $B \leftarrow g^b$ with $b = 42$. [3]

(iii) The following transcript of a conversation was intercepted, which contains a message encrypted with the ElGamal system (using the mapping from letters to numbers described above). 3

| | |
|---|---|
| Alice | has the public key $96034$. |
| Bob to Alice: | message (part 1) $(76441, 95649)$. |
| Bob to Alice: | message (part 2) $(76441, 56466)$. |
| Bob to Alice: | message (part 3) $(76441, 137012)$. |
| Bob to Alice: | message (part 4) $(76441, 63229)$. |

An indiscretion revealed that the third part of the message corresponds to the cleartext (value) $448$. Compute the (alphabetic) cleartext of the entire message.

**Exercise 10.3** (Reductions for RSA). (7+6 points)

We consider as an attacker a (probabilistic) polynomial-time computer $\mathcal{A}$. $\mathcal{A}$ knows pk $= (N, e)$ and $y = \text{enc}_{\text{pk}(x)}$. There are several notions of "breaking RSA". $\mathcal{A}$ might be able to compute from its knowledge one of the following data.

$B_1$: the plaintext $x$,

$B_2$: the hidden part $d$ of the secret key sk $= (N, d)$,

$B_3$: the value $\varphi(N)$ of Euler's totient function,

$B_4$: a factor $p$ (and $q$) of $N$.

If $A$ and $B$ are two computational problems (given by an input/output specification), then a *random polynomial-time reduction* from $A$ to $B$ is a random polynomial-time algorithm for $A$ which is allowed to make calls to an (unspecified) subroutine for $B$. The cost of such a call is the combined input plus output length in the call. If such a reduction exists, we write

$$A \leq_p B.$$

2 (i) Show that $B_1 \leq_p B_2$.

2 (ii) Show that $B_2 \leq_p B_3$.

2 (iii) Show that $B_3 \leq_p B_4$.

1 (iv) Which problem is the easiest one? Which one is most difficult?

+2 (v) Show that additionally we have $B_4 \leq_p B_3$. Hint: Consider the quadratic polynomial $(x-p)(x-q) \in \mathbb{Z}[x]$.

(vi) Argue that we also have $B_3 \leq_p B_2$. +4

(vii) Resolve the question whether also $B_2 \leq_p B_1$ or equivalently whether $B_4 \leq_p B_1$. Warning: This is an open research problem...