Cryptography, winter 2013/2014

PROF. DR. JOACHIM VON ZUR GATHEN, DR. DANIEL LOEBENBERGER

4. Exercise sheet
Hand in solutions until Saturday, 23 November 2013, 23:59:59

To solve the following exercises, you are strongly advised to use your favorite computer algebra system (or similar).

Exercise 4.1 (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 $a_0 + 26a_1 + 26^2 a_2$. 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 4.2 (Keys for the RSA system). (4+3 points)

Using the prime numbers $p = 13$ and $q = 11$ an RSA system is to be set up. (In practice these number would of course be much too small!!) Towards that end we choose $e = 17$ and $N = p \cdot q$ as our public key.

2 (i) Using the extended Euclidean algorithm, compute the corresponding private key d that satisfies: $e \cdot d = 1$ in $\mathbb{Z}_{(p-1)(q-1)}$.

1 (ii) Encrypt $x = 42$.

1 (iii) Decrypt $y = 48$.

+3 (iv) Use a programing language of sour choice to solve the exercise with the following numbers instead of the ones above:

$$\begin{aligned} p &= 2609899, \\ q &= 3004217, \\ e &= 54323425121, \\ x &= 4364863612562, \\ y &= 850080551629. \end{aligned}$$

Exercise 4.3 (Chinese Remainder Theorem). (6 points)

Consider two relatively prime positive integers $a, b \in \mathbb{Z}_{\geq 2}$ and the map

$$\varphi\colon \begin{array}{ccc} \mathbb{Z}_{ab} & \longrightarrow & \mathbb{Z}_a \times \mathbb{Z}_b, \\ x & \longmapsto & (x \bmod a, x \bmod b) \end{array}$$

In the set $\mathbb{Z}_a \times \mathbb{Z}_b$ we can add and multiply by performing the operations component-wise, i.e. we do computations modulo a in the first coordinate and modulo b in the second.

1 (i) Show that the map φ can be easily computed.

2 (ii) Explain how to construct two elements $x_a, x_b \in \mathbb{Z}_{ab}$ with $\varphi(x_a) = (0, 1)$ and $\varphi(x_b) = (1, 0)$.

2 (iii) Now consider an arbitrary element $(y, z) \in \mathbb{Z}_a \times \mathbb{Z}_b$. Using the previously computed values $x_a, x_b \in \mathbb{Z}_{ab}$, explain how to construct $x \in \mathbb{Z}_{ab}$ such that $\varphi(x) = (y, z)$. You might want to use the fact that φ is a homomorphism, i.e. preserves addition and multiplication.

1 (iv) Conclude that φ is an easily computable bijection between $\mathbb{Z}_{ab}$ and $\mathbb{Z}_a \times \mathbb{Z}_b$.