Homework 11 in Cryptography I

Prof. Dr. Rudolf Mathar, Michael Reyer, Henning Maier

14.07.2011

Exercise 36. [1]

Alice and Bob are using the Shamir's no-key protocol to exchange a message. They agree to use the prime $p = 31337$ for their communication. Alice chooses a random number $a = 9999$ while Bob chooses $b = 1011$. Alice's message is $m = 3567$.

(a) Carry out the protocol by calculating the inverses $a^{-1} \pmod{p-1}$ and $b^{-1} \pmod{p-1}$.

(b) Compute all messages with the given values.

Exercise 37.

Prove Proposition 8.3 from the lecture notes: Let $n = pq$, $p \neq q$ prime and x a nontrivial solution of $x^2 \equiv 1 \mod n$, i.e., $x \not\equiv \pm 1 \mod n$. Then

$$\gcd(x+1, n) \in \{p, q\}.$$

Exercise 38.

Alice is using the ElGamal encryption system for encrypting the messages m_1 and m_2. The generated cryptograms are

$$\mathbf{c}_1 = (1537, 2192) \text{ and } \mathbf{c}_2 = (1537, 1393).$$

The public key of Alice is $(p, a, y) = (3571, 2, 2905)$.

(a) What has Alice done wrong here?

(b) The first message is given as $m_1 = 567$. Determine the message m_2.

[1] **Remark**: For the calculation of the Square-And-Multiply Algorithm, you are free to use your computer