Homework 9 in Cryptography

Prof. Dr. Rudolf Mathar, Markus Rothe, Milan Zivkovic

17.07.2014

Exercise 31. Alice and Bob are using Shamir's no-key protocol to exchange a secret message. They agree to use the prime $p = 31337$ for their communication. Alice chooses the random number $a = 9999$ while Bob chooses $b = 1011$. Alice's message is $m = 3567$.

(a) Calculate all exchanged values c_1, c_2, and c_3 following the protocol.
Hint: You may use $6399^{1011} \equiv 29872 \pmod{31337}$.

Exercise 32. 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 33. Alice and Bob are using the ElGamal cryptosystem. The public key of Alice is $(p, a, y) = (3571, 2, 2905)$. Bob encrypts the messages m_1 and m_2 as

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

(a) Show that the public key is valid.

(b) What did Bob do wrong?

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