Homework 11 in Cryptography I

Prof. Dr. Rudolf Mathar, Wolfgang Meyer zu Bergsten, Michael Reyer

27.01.2009

Exercise 33. Suppose, Alice and Bob are using the Diffie-Hellman key agreement protocol with a prime $p = 376373$ and primitive root 2 modulo p as parameters. Alice uses the random number 21767, Bob uses 9973.

Conduct the key agreement protocol and compute the common key. What does Alice send to Bob, what does Bob send to Alice?

Exercise 34. Prove part b) of Theorem 7.2:
If there exists a primitive element modulo n then there are $\varphi(\varphi(n))$ many.

Exercise 35. 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 her random number $r_A = 9999$ while Bob chooses $r_B = 1011$. Alice's message is $m = 3567$.

Carry out the protocol by calculating the inverses $a^{-1} \pmod{p-1}$ and $b^{-1} \pmod{p-1}$. Then, compute all messages with the given values.