Homework 7 in Cryptography I

Prof. Dr. Rudolf Mathar, Paul de Kerret, Georg Boecherer

01.07.2009

Exercise 19. Suppose, Alice and Bob are using the Diffie-Hellman key agreement protocol with a prime $p = 376373$ and primitive element $a = 2$ modulo p as parameters. Alice uses the random number $r_A = 21767$, Bob uses $r_B = 9973$.

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

Exercise 20. 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. Particularly, compute all the messages sent by Alice and Bob, and verify that Bob receives the right message.

Exercise 21. Prove part b) of Theorem 7.2:
If there exists a primitive element modulo n then there exists $\varphi(\varphi(n))$ many.

Hint: Consider the elements of rank $\varphi(n)$ in the group $\mathbb{Z}_n^*$.