Cryptography

PROF. DR. JOACHIM VON ZUR GATHEN, KONSTANTIN ZIEGLER

6. Assignment: Diffie-Hellman key exchange and a derived public-key cryptosystem

(Due: Thursday, 10 December 2009, 23^{59})

Exercise 6.1 (Diffie-Hellman key exchange in $\mathbb{Z}_{20443}^{\times}$). (5 points)

ALICE and BOB want to agree on a common key over an insecure channel. To do so, they perform a Diffie-Hellman key exchange in the group $\mathbb{Z}_{20443}^{\times}$

(i) To find a generator for the cyclic group $\mathbb{Z}_{20443}^{\times}$, the following theorem is used: [2]

Theorem. *An element $a \in \mathbb{Z}_p^{\times}$ is a generator of $\mathbb{Z}_p^{\times}$ if and only if*

$$a^{(p-1)/t} \neq 1 \pmod{p}$$

for all prime divisors t of $p-1$.

Use this theorem to show that 2 is a generator of $\mathbb{Z}_{20443}^{\times}$.

(ii) Next, ALICE chooses her private key $a = 257$ and BOB chooses his private key $b = 1280$. What are the further steps, both sides have to perform, until they are both in possession of the common key, corresponding to their private keys? Do and document them. [3]

Exercise 6.2 (A public-key cryptosystem based on the Diffie-Hellman key exchange).

(18 points)

The Diffie-Hellman protocol for key exchange can be modified for a public-key cryptosystem to exchange messages. Let G be a finite cyclic group with d elements and generating element g:

- ALICE chooses her secret key $a \in_R \mathbb{Z}_d$ at random and publishes her public key $A = g^a \in G$.
- BOB chooses a temporary secret key $b \in_R \mathbb{Z}_d$ at random and computes his temporary public key $B = g^b$ as well as the temporary common key $k = A^b$.

- BOB encrypts the message $m \in G$ by computing $c = k \cdot m$.

(i) Which data must BOB send to ALICE and how can ALICE recover the original message m from that. [3]

[2] (ii) Discuss the correctness of this protocoll.

[4] (iii) Discuss the efficiency of this protocoll.

[5] (iv) Discuss the security of this protocoll by studying possible polynomial reductions to and from DH_G and DL_G. Use appropriate notations.

[4] (v) Let $G = \mathbb{Z}_{2579}^{\times}$ and $g = 2$. ALICE published as public key $A = 949$. You want to tell her the first three digits of your Student ID using as temporary secret $b = 17$. What data do you transmit? (

Note: You should be able to do all the involved computations using the calculator that you want to use in the final exam.