

Cryptography I, winter 2005/06  
JOACHIM VON ZÜR GATHEN, MICHAEL NÜSKEN

**8. Exercise sheet**

**Hand in before Monday, 2006/01/09, 14<sup>00</sup> in b-it 1.22.**

**Exercise 8.1** (Is it a generator? Find a generator?).

(4+2 points)

Let  $p$  be a prime number and  $G$  the group  $\mathbb{Z}_p^\times$  of units modulo  $p$ .

- (i) For  $a \in G$  holds:  $a$  is a generator of  $G$  if and only if  $a^{p-1} = 1$  and  $a^{(p-1)/t} \neq 1$  for all nontrivial divisors  $t > 1$  of  $p - 1$ . 1
- (ii) Furthermore: An element  $a \in \mathbb{Z}_p^\times$  is a generator if and only if  $a^{(p-1)/t} \neq 1 \pmod{p}$  holds for all prime divisors  $t$  of  $p - 1$ . 1
- (iii) Using this show that 2 is a generator of  $\mathbb{Z}_{20443}^\times$ . 1
- (iv) How would you compute a generator of a group  $\mathbb{Z}_p^\times$ ? 1
- (v) Suppose  $p - 1 = 2q$  with  $q$  prime. Find an element of order  $q$ . +1
- (vi) Suppose  $G$  is an abelian group with 15 elements. Find an element of order 7. +1

**Exercise 8.2** (ElGamal).

(2 points)

We implement the ElGamal cryptosystem using the unit group  $G = \mathbb{Z}_p^\times$  of integers modulo some prime  $p$ . A is mapped to 0, B to 1 and so forth, Z is mapped to 25. We combine groups of three letters  $(a_0, a_1, a_2)$  to  $a_0 + 26a_1 + 26^2a_2$ . Thus ABC corresponds to the value  $0 + 26 \cdot 1 + 2 \cdot 26^2 = 1378$ .

- (i) Encrypt the word "CHRISTMAS" using the ElGamal scheme. Use the group  $G = \mathbb{Z}_{20443}^\times$  and the generator  $g = 2$ . The receiver of the message has published the public key  $g^{s_A} = 8224$ . Choose your public key to be  $g^{s_B}$  with  $s_B = 321$ . 1
- (ii) The following transcript of a conversation was intercepted, which contains a message encrypted with the ElGamal system (using the mapping from letters to numbers described above). Once more we have  $G = \mathbb{Z}_{20443}^\times$  and  $g = 2$ : 1

Alice                      has the public key 7189.  
Bob to Alice:    message (part 1) (16278, 4151).  
Bob to Alice:    message (part 2) (12430, 4151).  
Bob to Alice:    message (part 3) (2689, 4151).

An indiscretion revealed that one part of the message corresponds to the clear text (value) 8324. Compute the (alphabetic) clear text of the entire message.

## Repetition

**Exercise 8.3** (A finite field).

(0+3 points)

Consider the finite field  $\mathbb{F}_{3^5} = \mathbb{F}_3[x] / \langle x^5 - x - 1 \rangle$ .

+1

(i) Add  $x^3 + x^2 + 1$  and  $x^4 + x + 1$  in  $\mathbb{F}_{3^5}$ .

+1

(ii) Multiply  $x^3 + x^2 + 1$  and  $x^4 + x + 1$  in  $\mathbb{F}_{3^5}$ .

+1

(iii) Calculate the inverse of  $x$  in  $\mathbb{F}_{3^5}$ .

**Exercise 8.4** (Modified RSA system).

(0+4 points)

The RSA system can be generalized to allow for products of more than two distinct prime numbers, and this modification is also used in practical implementations. Consider the RSA system for products  $N = p_1 \cdot p_2 \cdot p_3$  of three distinct primes:

**Algorithm.** 3RSA key generation.

1. Choose three distinct prime numbers  $p_1, p_2, p_3$ , so that

$$2^{n-1} < N = p_1 \cdot p_2 \cdot p_3 < 2^n.$$

2. Compute  $\varphi(N) = (p_1 - 1) \cdot (p_2 - 1) \cdot (p_3 - 1)$ .

3. Choose the public exponent  $e \in \{2, 3, \dots, \varphi(N) - 2\}$ , so that  $\gcd(e, \varphi(N)) = 1$ .

4. Compute the secret exponent  $d$ , so that  $d \cdot e \equiv 1 \pmod{\varphi(N)}$ .

5. Now  $(N, e)$  is the public key and  $(N, d)$  is the secret key.

Using these pairs of keys, the remainder of the system is identical to the one using products of two distinct primes.

+1

(i) Prove that the system works correctly.

+2

(ii) What are the advantages and disadvantages of this system? Consider the security and the efficiency.

+1

(iii\*) Try to generalize the RSA system to products  $N = p_1 \cdot p_2 \cdot \dots \cdot p_r$  of  $r$  primes. Are there noteworthy differences? (In practice values up to  $r = 5$  are being used.)

**Exercise 8.5** (Key size).

(0+3 points)

+1

(i) Determine upper and lower bounds, reasonably close to each other, on the number of keys and of messages for  $n$ -bit RSA as described in the course.

+2

(ii) The webpage <http://www.heidel-gmbh.de/Enigma2000.htm> advertises a cipher using a 4.5MBit key. By the enormous size of the key the developer makes the reader think that the system is highly secure. What do you think about it?

**Exercise 8.6** (Finding prime numbers).

(0+4 points)

- (i) Prove that  $\pi(2x) - \pi(x) > \frac{x}{2 \ln x}$  if  $x \geq e^6$ . *Hint*: Prime number theorem. +2
- (ii) Use (i) to give lower bounds on the number of  $k$ -bit primes for  $k = 16$ ,  $k = 32$  and  $k = 64$ . +1
- (iii) For  $k = 16$ , use a computer algebra system to count the primes between  $2^{15}$  and  $2^{16}$ . Compare with (ii). +1

**Exercise 8.7** (Small Public Exponent RSA Cryptosystem).

(0+6 points)

This exercise will show that when using the RSA system as a public key encryption scheme, small public exponents may be a real danger.

In a public domain the exponent  $e = 3$  is used as public exponent, thus every user chooses a public modulus  $N$  such that  $\gcd(\phi(N), 3) = 1$  and computes his respective secret exponent  $d$  such that  $3 \cdot d \bmod \phi(N) = 1$ . Suppose that the users  $A, B, C$  have the following public moduli:

$$N_1 = 5000746010773, N_2 = 5000692010527, N_3 = 5000296004107.$$

- (i) Alice sends a message  $m$  to  $A, B, C$  by encrypting:  $m_i = m^3 \bmod N_i$ . Eve intercepts and captures the following values: +3

$$m_1 = 1549725913504, m_2 = 2886199297672, m_3 = 2972130153144.$$

Show that Eve can recover the value of  $m$  without factoring  $N_i$  and compute this value with Maple. (Hint: Chinese Remainder Theorem)

- (ii) Generalize the method used by Eve above for general public exponent  $e$ . How many messages should Eve intercept in order to recover the clear text message? +1
- (iii) Suppose that RSA is used with a small public exponent  $e$  as an encryption scheme. Can a similar attack be used by Eve in order to create false signatures? Explain your answer. Remark:  $F_4 = 2^{16} + 1$  is very often used as a general public exponent in connection with the RSA scheme. +2

**Exercise 8.8** (Pollard's  $\varrho$  method).

(0+4 points)

Implement Pollard's  $\varrho$  algorithm for the discrete logarithm as presented in class and compute the discrete logarithm of your student registration number in the group  $\mathbb{Z}_p^\times$  with  $p = 10^6 + 3$  and base  $g = 2$ . Count the number of group operations needed and compare with the prediction from the lecture notes. +4

**We wish you nice holidays and a Happy New Year.**