Department of Mathematics
Stockholm University
Section: Mathematics
Examiner: Jonas Bergström

Exam
Mathematics of Cryptography
MM7018, 5 hp
2021-03-16 09:30–13:30

There are five problems on this written exam, each worth up to 9 points. These points will be assigned in conjunction with the accompanying oral exam, which will also feature additional problems for discussion. Altogether, these exams carry up to 85 points, which will be added to your points from the homework assignments. Grades are then given by the following preliminary intervals:

A: 100–92p, B: 91–84p, C: 83–76p, D: 75–68p, E: 67–60p.

Remember to motivate your answers carefully.

INSTRUCTIONS – **Read carefully!**

a) This exam is only valid taken in conjunction with an oral exam 2021-03-17, in accordance with the instructions emailed out to exam participants.

b) Allowed resources: You may use the course book and your course notes, and you are expected to use a calculator (in a limited way) in answering the questions. The calculator may be used to do:

- addition, subtraction, multiplication and division of two numbers,
- calculation of a residue modulo an integer, and
- calculation of a power a^b (potentially mod n).

Using computer software for the above purposes is allowed, but only for the above operations.

c) You need to include all the steps and write motivation in your solutions, or you will not receive points for them. Wherever you have used a calculator to do a computation, you need to indicate this specifically, say by writing for example "CALC($\times 2$)" or "CALC($+$)" above an equals sign.

d) You may not have any communication with anyone else during the exam, whether verbal or written, sending or receiving, except for the examiner.

e) On the first page of your answer submission, write the total number of submitted pages and the following declaration, appropriately filled in, and sign your agreement to it:

I, __name__, declare that that the answers submitted in my name are written by me, and were arrived at without input from anyone else, using only the allowed resources.

__Signature__, *person number*

f) You must submit your solutions as a **single PDF** on the course web page, by 14:15 at the latest.

Questions

1. (a) (2p) In this question you may **not** use the calculator to compute powers a^b, except when $b = 2$. Use fast powering to compute $93^{840} \pmod{197}$. Give your answer as an integer in $\{0, 1, 2, \ldots, 196\}$.

   (b) (4p) Let p be prime number and e be an integer. Give an expression (in terms of p, e) for how many solutions (modulo p) there are to the equation

   $$x^e \equiv_p 1,$$

   and prove that it holds.

   (c) (3p) The element 2 is a primitive root in $\mathbb{F}_{101}^*$. Determine all integer solutions to

   $$32^x \equiv_{101} 14.$$

2. (a) (3p) Let $N = 3233$. Choose an integer a and make one Miller-Rabin test and determine if the chosen a is a witness for N.

   (b) (6p) Use the Pohlig-Hellman algorithm to solve the following DLP:

   $$7^x \equiv_{71} 64.$$

3. (a) (2p) Consider the elliptic curve

   $$E : y^2 = x^3 + x + 4 \quad \text{over } \mathbb{F}_{13}.$$

   The points $P = (8, 2)$ and $Q = (7, 9)$ lie on the curve. Compute $P + Q$ on E, showing all your steps.

   (b) (3p) The elliptic curve $E : y^2 = x^3 + 6x + 1$ over $\mathbb{F}_{211}$ has 202 points. Find a point on E has order 101.

   (c) (4p) Say that we want to use Lenstra's factorization algorithm to factor $N = 60551$, and that three different values of (A, a, b), namely (A_1, a_1, b_1), (A_2, a_2, b_2), and (A_3, a_3, b_3) are given, from which one can compute $P = (a, b)$ and $B \equiv_N b^2 - a^3 - A \cdot a$. Determine for which of these three values Lenstra's factorization algorithm will finish and give a non-trivial factor of N first.

   Use the information that $N = pq$ with $p = 151$ and $q = 401$, and that the elliptic curve $E : y^2 = x^3 + Ax + B$ has

   i. 154 points over $\mathbb{F}_p$ and 410 points over $\mathbb{F}_q$ when $(A, a, b) = (A_1, a_1, b_1)$,
   ii. 162 points over $\mathbb{F}_p$ and 405 points over $\mathbb{F}_q$ when $(A, a, b) = (A_2, a_2, b_2)$,
   iii. 130 points over $\mathbb{F}_p$ and 435 points over $\mathbb{F}_q$ when $(A, a, b) = (A_3, a_3, b_3)$

   and that in all these cases P is a generator of the elliptic curve.

4. (9p) Let $p = 37$, $g = 5$ (a primitive root in $\mathbb{F}_p^*$), and $h = 23$. This question is about solving the DLP

$$g^x = h \quad \text{in } \mathbb{F}_p^*$$

using information obtained from iterates of the map f defined by

$$f(x) = \begin{cases} gx \bmod p & \text{if } 0 \le x < 12 \\ x^2 \bmod p & \text{if } 12 \le x < 24 \\ hx \bmod p & \text{if } 24 \le x < 37. \end{cases}$$

Let $x_0 = y_0 = 1$, and define $x_{i+1} = f(x_i)$ and $y_{i+1} = f(f(y_i))$. Within a few steps of computing these, one finds a coincidence $x_k = y_k$. Find this coincidence, and use it to solve the above-mentioned DLP.

5. (a) (3p) Let $N = 1769461$, $F(T) = T^2 - N$ and $a = \lfloor \sqrt{N} \rfloor + 1 = 1330$. Characterize for which $k \ge 0$ the numbers of the form $F(a+k)$ that are divisible by 19 and which that are divisible by 23.

   (b) (4p) Take the same $a, N, F(T)$. After computing $F(a+i)$ for i from 0 to 6000 we find the following seven 11-smooth numbers:

$$(a+1)^2 - N = 2^2 \cdot 3 \cdot 5^2 \cdot 7, \tag{1}$$
$$(a+6)^2 - N = 3^2 \cdot 5 \cdot 7^3, \tag{2}$$
$$(a+286)^2 - N = 3^7 \cdot 5 \cdot 7 \cdot 11, \tag{3}$$
$$(a+421)^2 - N = 2^2 \cdot 3^3 \cdot 5 \cdot 7^4, \tag{4}$$
$$(a+3289)^2 - N = 2^2 \cdot 3 \cdot 5^2 \cdot 7^2 \cdot 11^3, \tag{5}$$
$$(a+4389)^2 - N = 2^2 \cdot 3^2 \cdot 5^7 \cdot 11, \tag{6}$$
$$(a+5951)^2 - N = 2^2 \cdot 5^3 \cdot 7 \cdot 11^4. \tag{7}$$

   How many perfect squares can one can form out of these numbers? Write out two perfect squares (formed out of these numbers) explicitly.

   (c) (2p) Use the two perfect squares formed in part (b) to check for factors of N.