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

Exam
Mathematics of Cryptography
MM7018, 5 hp
2021-04-20 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 2021-04-21, 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(×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) Use the Chinese remainder theorem to find all integer solutions to the following system of equations:

$$\begin{cases} 3x \equiv 5 \mod 7 \\ 3x \equiv 4 \mod 10 \\ 7x \equiv 19 \mod 27 \end{cases}$$

   (b) (3p) Say that $N = p_1^{r_1} \cdot \ldots \cdot p_k^{r_k}$ where $p_1, \ldots, p_k$ are distinct primes and that G is a group with N elements. Show that an element $g \in G$ is a generator of G if and only if $g^{N/p_i} \neq 1$ for all $i = 1, \ldots, k$.

   (c) (4p) Say that $p \equiv_4 3$. Fix any $a \not\equiv_p 0$. Show that if the equation $x^2 \equiv_p a$ has a solution, then its solutions are $a^{(p+1)/4}$ and $-a^{(p+1)/4}$. Show furthermore that if the equation $x^2 \equiv_p a$ does not have a solution then $a^{(p+1)/2} \equiv_p -a$.

2. (a) (2p) Let $N = 28409$. Make one Miller-Rabin test and determine if $a = 5$ is a witness for N.

   (b) (3p) Find all integer solutions to the equation

$$x^{77} \equiv_{221} 11.$$

   (c) (4p) Use Shanks's baby-step giant-leap algorithm to solve the following DLP:

$$11^x \equiv_{47} 41.$$

3. (a) (2p) Find all points on the elliptic curve defined by

$$y^2 = x^3 + x + 4 \quad \text{over } \mathbb{F}_{17}.$$

   (b) (3p) Find all points of order 2 on the elliptic curve defined by $E : y^2 = x^3 - x$ over $\mathbb{F}_{37}$. Use this to determine if the group of points is cyclic or not.

   (c) (4p) Say that we want to use Lenstra's factorization algorithm to factor $N = 64213$, 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 $p = 157$ and $q = 409$, and that the elliptic curve $E : y^2 = x^3 + Ax + B$ has

   i. 151 points over $\mathbb{F}_p$ and 401 points over $\mathbb{F}_q$ when $(A, a, b) = (A_1, a_1, b_1)$,
   ii. 160 points over $\mathbb{F}_p$ and 406 points over $\mathbb{F}_q$ when $(A, a, b) = (A_2, a_2, b_2)$,
   iii. 156 points over $\mathbb{F}_p$ and 408 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 E be the elliptic curve defined by

$$y^2 = x^3 + 2x + 3 \quad \text{over } \mathbb{F}_{107},$$

which has 102 points. Use the Pohlig-Hellman algorithm to solve the DLP

$$xP = Q,$$

where $P = (4, 17)$ and $Q = (47, 39)$. The following table will be useful

$$\begin{pmatrix} P & 2P & 4P & 8P & 16P & 32P & 64P \\ (4,17) & (36,87) & (3,101) & (63,44) & (28,66) & (51,41) & (91,35) \end{pmatrix}$$

5. (a) (3p) Let $N = 1557739$, $F(T) = T^2 - N$ and $a = \lfloor\sqrt{N}\rfloor + 1 = 1249$. Characterize for which $k \geq 0$ 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 3000 we find the following six 13-smooth numbers:

$$(a+59)^2 - N = 5^5 \cdot 7^2, \tag{1}$$
$$(a+154)^2 - N = 2 \cdot 3^5 \cdot 5 \cdot 13^2, \tag{2}$$
$$(a+559)^2 - N = 3^4 \cdot 5^3 \cdot 13^2, \tag{3}$$
$$(a+1168)^2 - N = 2 \cdot 3 \cdot 5^2 \cdot 13^4, \tag{4}$$
$$(a+2098)^2 - N = 2 \cdot 3^9 \cdot 5 \cdot 7^2, \tag{5}$$
$$(a+2343)^2 - N = 3^3 \cdot 5^2 \cdot 7^5, \tag{6}$$

   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.