Department of Mathematics
Stockholm University
Section: Mathematics
Examiner: Olof Sisask

Exam
Mathematics of Cryptography
MM7018, 7.5 hp
2020-04-15 09:30–13:30

There are six problems on this written exam, each worth up to 8 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 80 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 2020-04-16, 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
- *where explicitly stated in the question,* 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. In this question you may **not** use the calculator to compute powers a^b, except when $b = 2$.

   (a) (2p) Compute $93^{840} \pmod{211}$. Give your answer as an integer in $\{0, 1, 2, \ldots, 210\}$. If you appeal to a theorem, make sure you fully justify why its hypotheses are satisfied.

   (b) (2p) Compute $5^{1029} \pmod{3000}$. Give your answer as an integer in $\{0, 1, 2, \ldots, 2999\}$. If you appeal to a theorem, make sure you fully justify why its hypotheses are satisfied.

   (c) (2p) The element 3 is a primitive root in $\mathbb{F}_{127}^*$. Determine all integer solutions to

   $$27^x \equiv 94 \pmod{127}.$$

   (d) (2p) Consider the elliptic curve

   $$E : y^2 = x^3 + 3 \quad \text{over } \mathbb{F}_{11}.$$

   The point $P = (1, 2)$ lies on the curve. Compute $P + P$ (on E), showing all your steps.

2. In this question you may **not** use the calculator to compute powers a^b, except when $b = 2$.

   (a) (2) What is the order of the element 2 in the group $\mathbb{F}_{29}^*$? (Motivate!)

   (b) (4) Use Shanks's Babystep–Giantstep algorithm to solve the discrete logarithm problem

   $$2^x = 13$$

   in the group $\mathbb{F}_{29}^*$, making all parameter choices and steps clear.

   (c) (1) In the group $(\mathbb{Z}/1013\mathbb{Z}, +)$, what is the order of the element 2? (Note that the group operation is *addition*.)

   (d) (1) In the same group $(\mathbb{Z}/1013\mathbb{Z}, +)$, compute $\log_2(57)$ and $\log_2(114)$. (Note that the group operation is *addition*.)

3. In this question you may use the calculator to compute powers a^b.

   Let $p = 83$ (a prime). The element $g = 2$ is a primitive root in $\mathbb{F}_p^*$. This question is about the ElGamal digital signature scheme in this group.

   (a) (2p) Let $a = d + 3$, where d is the last digit of your person number. Create a public verification key based on secret signing key a, and create a signature for the document 10. ('Random' choices may be determined however you please.)

   (b) (3p) Samantha has ElGamal public verification key 11. Cliff claims that Samantha has signed the documents $D = 10$ and $D' = 20$, with corresponding signatures

   $$(S_1, S_2) = (5, 2) \quad \text{and} \quad (S_1', S_2') = (5, 4).$$

   Determine which of the documents Samantha actually signed (if any).

   (c) (3p) One should not reuse the same random element in ElGamal digital signature creation for different documents. Explain how one can see that this advice was not followed in the following scenario, and exploit this to find the secret signing key: the two documents $D = 7$ and $D' = 34$ were signed with the same secret signing key and produced the corresponding signatures

   $$(S_1, S_2) = (5, 11) \quad \text{and} \quad (S_1', S_2') = (5, 12).$$

4. In this question you may use the calculator to compute powers a^b.

   (a) (4p) Let $p = 577$ (a prime). The element $g = 25$ has order 288 in $\mathbb{F}_p^*$. Let $h = 251$. Use the Pohlig–Hellman algorithm to solve the DLP

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

   (b) (4p) Let $p = 251$ (a prime) and let $q = 5$. The element $g = 3$ has order $q^3 = 125$ in $\mathbb{F}_p^*$. Use the Pohlig–Hellman algorithm to solve the DLP

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

   where $h = 15$.

5. In this question you may use the calculator to compute powers a^b.

   (a) (3p) Suppose you know that the integer N has the prime factorisation $N = pq$. Suppose $p = 2^8 + 1$ and $q = 2r + 1$ for a prime r with 1000 digits. Name an algorithm from the course that is likely to be able to find the factorisation of N fairly quickly, and carry out the algorithm in a 'baby case' where $r = 29$. (Tip: if you need to compute GCDs, you are allowed to use that you know the factorisation of N in this particular question.)

   (b) (5p) Let $p = 31$, $g = 3$ (a primitive root in $\mathbb{F}_p^*$), and $h = 10$. 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

   $$f(x) = \begin{cases} gx \bmod p & \text{if } 0 \leq x \leq 10 \\ x^2 \bmod p & \text{if } 11 \leq x \leq 20 \\ hx \bmod p & \text{if } 21 \leq x \leq 30. \end{cases}$$

   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.

6. In this question you may use the calculator to compute powers a^b.

   (a) (1p) Describe a practical cryptographic use for the Miller–Rabin test, other than RSA.

   (b) (2p) Let $n = 341$. Which of the following values of a are Miller–Rabin witnesses for the compositeness of the integer n? (Motivate clearly!)

   $$a : 2, 3, 4.$$

   (c) (5p) Let n be a product of two primes, and assume that $n = 4k + 1$ where k is an odd integer. Suppose that the integer a is *not* a Fermat-witness for the compositeness of n. This means that

   $$a^{n-1} \equiv 1 \pmod{n}.$$

   Suppose further that a *is* a Miller–Rabin witness for the compositeness of n. Show how one can use this witness a to efficiently find the prime factorisation of n. Demonstrate your method by applying it to factorise n from part (a). (Hint: factorise $a^{n-1} - 1$.)