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.

Solution: (a) Ans: 1. Must check that 211 is a prime.

(b) Ans: 125. Note: $5^3 = 625$, and $625^2 \equiv 625 \pmod{3000}$. Also $1029 = 1024 + 4 + 1$.

(c) Ans:

$$x = 2 + 42k, \quad k \in \mathbb{Z}.$$

Note: $27^2 \equiv 94 \pmod{127}$

(d) Ans: On this curve, if $Q = (x, y)$ then $Q + Q$ can be calculated by letting

$$\lambda = \frac{3x^2}{2y}$$

and $Q + Q = (x', y')$, where

$$x' = \lambda^2 - 2x \quad \text{and} \quad y' = \lambda(x - x') - y.$$

For us,

$$\lambda = \frac{3}{4} = 3 \cdot 3 = 9,$$

and so

$$P + P = (2, -9 - 2) = (2, 0).$$

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*.)

Solution: (a) Ans: 28. Since $28 = 4 \cdot 7$, it suffices to check that $2^{14} \neq 1$, and $2^4 \neq 1$.

(b) The order of 2 is $N = 28$, so we let $n = 1 + \lfloor \sqrt{N} \rfloor = 6$, and compute two lists: $1, g, g^2, \ldots, g^n$ and $h, hg^{-n}, hg^{-2n}, \ldots, hg^{-n^2}$, yielding

$$1, 2, 4, 8, 16, 3, 6$$

and

$$13, 7, 6, \ldots$$

Having found this collision, we can stop, knowing that

$$g^n = 6 = hg^{-2n},$$

whence

$$h = g^{18}.$$

(c) Since $\gcd(1013, 2) = 1$, the element 2 has order 1013: if $2x \equiv 0 \pmod{1013}$, then $x \equiv 0 \pmod{1013}$.

(d) $\log_2(57)$ is given by the solution to

$$2x \equiv 57 \pmod{1013}.$$

Since $2^{-1} \equiv (1013 + 1)/2 \equiv 507 \pmod{1013}$, this gives

$$\log_2(57) = x \equiv 57 \cdot 507 \equiv 535.$$

Furthermore,

$$\log_2(114) = 2 \log_2(57) = 57.$$

(Alternatively, just note that $2 \cdot 57 = 114$.)

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

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

Solution: (a) The public verification key is given by $A = g^a \bmod p$, which depends on d as follows:

d	0	1	2	3	4	5	6	7	8	9
A	8	16	32	64	45	7	14	28	56	29

For the signature, one needs to pick an integer k with $1 < k < p$ such that $\gcd(k, p-1) = 1$, and compute

$$S_1 = g^k \bmod p$$
$$S_2 = (D - aS_1)k^{-1} \bmod (p-1).$$

It is important here that k^{-1} is computed mod $(p-1)$, not p.

To verify that these have been computed correctly, we can check $A^{S_1} S_1^{S_2} \equiv g^D \pmod{p}$, where $g^D = 2^{10} \equiv 28 \pmod{p}$.

(b) We need to compute $A^{S_1} S_1^{S_2} \bmod p$ for each of the signatures, and compare this to $g^D \bmod p$ for the corresponding document.

We have

$$A^{S_1} = 11^5 \equiv 31 \pmod{p}.$$

We also have

$$S_1^{S_2} = 5^2 = 25,$$

and so for the first signature we have

$$A^{S_1} S_1^{S_2} \equiv 31 \cdot 25 \equiv 28 \pmod{p}.$$

We compare this to

$$g^D = 2^{10} \equiv 28 \pmod{p}.$$

Since these are equal mod p, we have verified that the signature for D is correct.

For the second document, we have the same value of $A^{S_1'}$, but now

$$S_1'^{S_2'} = 5^4 \equiv 44 \pmod{p},$$

and so

$$A^{S_1'} S_1'^{S_2'} \equiv 31 \cdot 44 \equiv 36 \pmod{p}.$$

For the document we have

$$g^{D'} = 2^{20} \equiv 37 \pmod{p}.$$

Since these are different, Samantha's key did not produce this signature for D'.

(c) Let a be the secret signing key we are after. Since $S_1 = S_1'$ and g is a primitive root, the same random element k was used to create both signatures. From the definition of S_2 and S_2', this means that

$$11 \equiv (7 - 5a)k^{-1} \pmod{82}$$
$$12 \equiv (34 - 5a)k^{-1} \pmod{82}.$$

Multiplying each of these by k (which is invertible) and subtracting the first from the second yields

$$k = 27.$$

Substituting this into the second (multiplied) equation we get

$$12 \cdot 27 \equiv 34 - 5a \pmod{82},$$

which since $12 \cdot 27 = 4 \cdot 81 \equiv -4 \pmod{82}$ is equivalent to

$$a \equiv 5^{-1}(34 + 4) \equiv 33 \cdot 38 \equiv 24 \pmod{82}.$$

The secret key was thus 24.

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 $h = 15$.

Solution: (a) Ans: $x = 65$ Write $N = 288 = 2^5 3^2$. Following the Pohlig–Hellman algorithm, set

$$g_1 = g^{N/2^5} = g^9 = 400$$
$$h_1 = h^{N/2^5} = h^9 = 400$$

and

$$g_2 = g^{N/3^2} = g^{2^5} = 335$$
$$h_2 = h^{N/3^2} = h^{2^5} = 287.$$

In the first stage of the algorithm, we need to find solutions y_1, y_2 to

$$g_1^{y_1} = h_1, \qquad g_2^{y_2} = h_2.$$

We see immediately that $y_1 = 1$ is a solution to the first equation. For the second one, we need only consider the possibilities $y_2 \in \{0, 1, 2, \ldots, 8\}$ as g_2 has order 3^2. We find quickly that $y_2 = 2$ is a solution.
The second stage of the algorithm says that the solution x to the original DLP can be found as the solution to the system

$$x \equiv y_1 \equiv 1 \pmod{2^5}, \qquad x \equiv y_2 \equiv 2 \pmod{3^2},$$

which we can solve by the Chinese Remainder Theorem. The first congruence is equivalent to $x = 1 + 2^5 k$, $k \in \mathbb{Z}$, from which the second congruence is equivalent to $2^5 k \equiv 1 \pmod{3^2}$. Since $2^5 \equiv 5 \pmod 9$, and $5^{-1} \equiv 2 \pmod 9$, this is equivalent to $k \equiv 2 \pmod{3^2}$. The full set of solutions is thus given by, for arbitrary $m \in \mathbb{Z}$,

$$x = 1 + 2^5(2 + 3^2 m) = 65 + 288m.$$

Taking $m = 0$ yields the solution $x = 65$ to the DLP.

(b) Ans: $x = 1 + q + 2q^2 = 56$. As in the algorithm, we write $x = x_0 + x_1 q + x_2 q^2$ with $0 \le x_i \le q - 1$ (that is, $0 \le x_i \le 4$) and try to determine first x_0, then x_1 and then finally x_2.
If $g^x = h$, then since g has order q^3 we must have

$$g^{q^2 x_0} = g^{q^2 x} = h^{q^2}.$$

Here

$$g^q = 3^5 = 243 = -8,$$

so

$$g^{q^2} = (-8)^5 = -138 = 113.$$

Also

$$h^{q^2} = 15^{5^2} = 100^5 = 113.$$

Thus, if there is a solution x, it must have $\boxed{x_0 = 1}$, which we henceforth set.
It follows that

$$g^{x_1 q + x_2 q^2} = hg^{-1} = 15 \cdot 84 = 5,$$

the inverse of 3 modulo 251 being $252/3 = 84$. Raising this equation to the power of q, we see that

$$g^{x_1 q^2} = 5^{q^2}.$$

We already know that $q^{q^2} = 113$, and a calculation yields $5^q = 113$. Hence $\boxed{x_1 = 1}$ as well.
It follows that

$$g^{x_2 q^2} = hg^{-1}g^{-q} = 5 \cdot (-8)^{-1}.$$

Using the Extended Euclidean algorithm we determine $8^{-1} = -94$, and so the above equation yields

$$113^{x_2} = 5 \cdot 94 = 219.$$

Clearly $x_2 = 0$ and $x_2 = 1$ do not work. A quick calculation confirms that $113^2 = 219$, however, whence $\boxed{x_2 = 2}$.
According to the algorithm, the solution to the DLP is given by

$$x = 1 + q + 2q^2 = 56.$$

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

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

   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.

Solution: (a) Since $p - 1$ has only small prime factors (namely 2, to a reasonably small power), Pollard's $p - 1$ method is appropriate.

(b) One gets $x_4 = y_4$:

i	x_i	y_i	$f(y_i)$	Computations		
0	1	1	3			$f(y_0) = g$
1	3	9	27	$x_1 = g$	$y_1 = f(f(y_0)) = g^2$	$f(y_1) = g^3$
2	9	22	3	$x_2 = g^2$	$y_2 = f(f(y_1)) = f(g^3) = g^3 h$	$f(y_2) = g^3 h^2$
3	27	9	27	$x_3 = g^3$	$y_3 = f(f(y_2)) = f(g^3 h^2) = g^4 h^2$	$f(y_3) = g^5 h^2$
4	22	22	3	$x_4 = g^3 h$	$y_4 = f(f(y_3)) = f(g^5 h^2) = g^5 h^3$	

The collision $x_4 = y_4$ thus yields

$$\begin{aligned} & g^3 h = g^5 h^3 \\ \iff \quad & h^2 = g^{-2}. \end{aligned}$$

Since $h = g^x$, this implies that $2x \equiv -2 \pmod{30}$, since g has order 30, which is equivalent to

$$x \equiv -1 \pmod{15}.$$

Thus the only possibilities for x are 14 and -1. A quick check yields that x is not -1, so $x = 14$. (We know a solution exists, since g is a primtive root.)

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 $a^{n-1} - 1$.)

Solution: (a) For example in finding the large primes that are needed for the ElGamal cryptosystem or digital signature scheme.

(b) We have that $n - 1 = 340 = 2 \cdot 170 = 2^2 \cdot 85$. Let us write $k = 85$. By definition, a number a with $\gcd(a, n) = 1$ is then a Miller–Rabin witness for n if all the following conditions are satisfied:

i. $a^k \not\equiv \pm 1 \pmod{n}$

ii. $a^{2k} \not\equiv -1 \pmod{n}$.

In our cases we have

a	$a^k \bmod n$	$a^{2k} \bmod n$
2	32	1
3	254	67
4	1	$*$

Thus $a = 2$ and $a = 3$ are Miller–Rabin witnesses for n, and $a = 4$ is not.

(c) Since $n = 4k + 1$, the definition of a being a Miller–Rabin witness for n is exactly as above. In other words,

- $a^k - 1 \not\equiv 0 \pmod{n}$
- $a^k + 1 \not\equiv 0 \pmod{n}$
- $a^{2k} + 1 \not\equiv 0 \pmod{n}$.

On the other hand, since a is not a Fermat-witness for n, we have

$$0 \equiv a^{n-1} - 1 = a^{4k} - 1 = (a^{2k} - 1)(a^{2k} + 1) = (a^k - 1)(a^k + 1)(a^{2k} + 1) \pmod{n}.$$

Thus, if $n = pq$ is the prime factorisation of n, then p must divide at least one of the factors

$$(a^k - 1), \quad (a^k + 1), \quad (a^{2k} + 1),$$

and so too must q. By the conditions on a above, from a being a Miller–Rabin witness, it cannot be the case that both p and q divide the same factor. Thus we can recover p and q by computing

- $\gcd(a^k - 1, n)$
- $\gcd(a^k + 1, n)$
- $\gcd(a^{2k} + 1, n)$,

each of which is a fast operation, by fast powering. At least one of these will be p, and at least one will be q.

Demonstration from (a):
Taking $a = 2$ from part (a), this not being a Fermat-witness for $n = 341$, we compute

$$\gcd(a^k - 1, n) = \gcd(31, 341) = 31.$$

Since $341/31 = 11$, we have found our prime factorisation. (The second factor, 11, can also be found via a gcd-computation as above.)