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

Exam
Mathematics of Cryptography
MM7018, 7.5 hp
2020-03-16 09:00–14:00

There are ten problems, each giving between 0 and 8 points. The points from the exam are added to your points from the homework assignments. Grades are then given by the following intervals:

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

Remember to motivate your answers carefully. You may use Big-O notation unless explicit constants are asked for. No calculators or computers may be used.

Try to keep your answers concise; no question is asking for an essay.

1. (a) (2p) Describe the basic framework for a private key (symmetric) cryptosystem.
   (b) (2p) Describe the basic framework for a public key cryptosystem. Mention, in particular, what a one-way function with trapdoor information is, and its role in the system.
   (c) (1p) State some of the main advantages of public key cryptosystems relative to private key cryptosystems, and vice versa. (Short explanations suffice.)
   (d) (3p) Explain the essential properties that a practical cryptosystem must have when it comes to speed of computation. What does it mean for a system to be secure against a *known plaintext attack*? What does it mean to be secure against a *chosen plaintext attack*? (You may answer in the context of either symmetric or asymmetric cryptosystems.)

2. (a) (1p) Show the steps used by the Euclidean algorithm to compute $\gcd(55, 34)$.
   (b) (2p) Describe the Euclidean algorithm for computing $\gcd(a, b)$, where $a \geq b \geq 1$ are integers.
   (c) (3p) Prove that the algorithm terminates in at most $2 + 2\log_2 b$ division steps.
   (d) (2p) Prove that the algorithm needs at least $\log_2 b$ division steps for infinitely many integers b. Hint: let $a_0 = 1$, $a_1 = 1$ and $a_{k+1} = a_k + a_{k-1}$, for $k \geq 1$, be the Fibonacci sequence. Analyse how the Euclidean algorithm performs when computing $\gcd(a, b)$ for $a = a_{n+1}$, $b = a_n$. (You do not need to use the most accurate relationship between n and b to prove the stated bound; a simple one will do.)

3. (a) (2p) Compute $3^{129} \pmod{6480}$. Give your answer as an integer in $\{0, 1, 2, \ldots, 6479\}$.
   (b) (2p) Compute $5^{601} \pmod{151}$. Give your answer as an integer in $\{0, 1, 2, \ldots, 150\}$. If you use a theorem, make sure you justify why its hypotheses are satisfied.
   (c) (2p) Determine all integer solutions to the system of congruences

$$\begin{cases} 4x \equiv 2 \pmod{15} \\ x \equiv 3 \pmod{49}. \end{cases}$$

   (d) (2p) The element 2 is a primitive root in $\mathbb{F}_{53}^{\times}$. Determine all integer solutions to

$$4^x \equiv 11 \pmod{53}.$$

4. Let G be a finite group, and let $g \in G$.

   (a) (1p) Describe what is meant by a Discrete Logarithm Problem (DLP) to base g in G.

   (b) (3p) Describe Shanks's Babystep–Giantstep Algorithm for solving a DLP in G. (You do not need to prove that the algorithm works.)

   (c) (1p) In how many steps does this algorithm guarantee to solve the DLP? How much storage does it need in general? Relate your answers to part (b).

   (d) (1p) What is the main advantage of Pollard's ρ method over Shanks's method for solving the DLP in $\mathbb{F}_p^\times$? Is there a disadvantage?

   (e) (2p) If the group is $(\mathbb{Z}/N\mathbb{Z}, +)$ (that is, with addition as the group operation) and g is relatively prime to N, explain how the DLP to base g can be solved very quickly.

5. (a) (2p) Describe a practical use for digital signature schemes.

   (b) (4p) Describe all the steps in any one specific digital signature scheme from the course.

   (c) (2p) Describe what hashing is, and its role in digital signature creation.

6. (a) (2p) State the Pohlig–Hellman theorem on the number of steps needed to solve a DLP to a base g, when the order N of g is known to factor as $N = q_1^{e_1} q_2^{e_2} \cdots q_t^{e_t}$, where the q_i are distinct primes. (Make sure you state in which setting the theorem applies.)

   (b) (2p) Suppose you wish to pick a prime p and a primitive root in $\mathbb{F}_p^\times$ for use as a base for a DLP. What implications does the Pohlig–Hellman theorem have for your choices if you want the DLP to be secure?

   (c) (4p) Let G be a group, and q a prime. Suppose you have an algorithm that can solve the DLP in G to any base of order q in S_q steps. Let $g \in G$ be an element of order q^2. Prove that you can solve any DLP in G to base g in $O(S_q)$ steps.

7. (a) (3p) Suppose Alice wants to receive secure, encrypted messages from others using the RSA cryptosystem. Describe what she needs to do to set this up, including how she can decrypt encrypted messages. Explain why the decryption process works. (You may assume theorems from modular arithmetic.)

   (b) (2p) What is the mathematical problem underpinning the security of RSA, according to the best approaches known? Specify the running time for one of the two best methods known for solving this problem. Classify whether it is exponential, subexponential or polynomial.

   (c) (3p) Describe the Miller–Rabin test and how it can be used to help generate some of the public parameters involved in RSA. If your description involves randomisation, justify why the probability of success is high.

8. (a) (7p) Let $p = 503$ (a prime), $g = 53$ and $h = 204$. The element g is a primitive root modulo p. Solve $g^x \equiv h \pmod{p}$ using index calculus.

   The fact that $hg^{-88} \equiv 60 \pmod{p}$ and the following table might be helpful.

i	$g^i \pmod{p}$
457	$3^4 \cdot 5$
434	$3^3 \cdot 7$
136	$3^2 \cdot 7$
12	$2 \cdot 3^3$

   (b) (1p) Say briefly how a table such as the above might be found in practice, and in particular why one is likely to have success in doing so.

9. (a) (2p) Name two different ways in which elliptic curves are relevant to modern cryptography.

   (b) (1p) Consider the elliptic curve over $\mathbb{F}_p$ ($p \geq 5$) given by

   $$E : y^2 = x^3 + 3.$$

   What does the Hasse bound say about the number of points of $E(\mathbb{F}_p)$?

   (c) (2p) With E as above, how many points does $E(\mathbb{F}_7)$ have? How does this compare to the bound from the previous part?

   (d) (3p) Describe how elliptic curve Diffie–Hellman key exchange works. Explain why it is not truly necessary for Alice and Bob to transmit the full pair (x, y) defining a point at each step, and why not doing so could be advantageous. (You may assume that we are working over a prime field $\mathbb{F}_p$ with $p \equiv 3 \pmod 4$.)

10. (a) (2p) Describe briefly the relationship between Pollard's $p - 1$ method and Lenstra's elliptic curve factorisation method. (You do not have to describe in detail how either one works.)

    (b) (2p) What is the expected running time of Lenstra's elliptic curve factorisation method in factorising N, if $N = pq$ is a product of two primes and $p < q$? Under what circumstances might this offer an advantage over the other factorisation methods of the course?

    (c) (4p) This question is about finding a factor of the number $N = 2021 = 43 \cdot 47$ using Lenstra's method. Consider the equation

    $$E : y^2 = x^3 + 3x - 3$$

    defining an elliptic curve over various fields. The curve contains the point $P = (1, 1)$ over any field, and over $\mathbb{Z}/N\mathbb{Z}$. It turns out that

    $$11P = \mathcal{O} \text{ over } \mathbb{F}_{43},$$
    $$37P = \mathcal{O} \text{ over } \mathbb{F}_{47},$$

    and that 11 and 37 are the smallest such numbers.

    Describe how Lenstra's algorithm will run, motivating why it will find a non-trivial factor of N and stating after how many steps.

The exam will be returned 11.00–11.45 on Friday 27 March in room 112 in house 6. After that it can be collected in room 204 in house 6.