MATEMATISKA INSTITUTIONEN
STOCKHOLMS UNIVERSITET
Avd. Matematik
Examinator: Jonas Bergström

Tentamensskrivning i
Mathematics of Cryptography, 7,5 hp
18 March 2019
9.00-14.00

There are ten problems, each giving between 0 and 8 points. The points from the exam is added to 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. No calculators or computers may be used.

1. a) Explain what a public key cryptosystem is. In particular, explain what a one-way-function with a trapdoor is, and its function in a public key cryptosystem. 2 p

   b) Describe the problem one needs to solve to decrypt a ciphertext of the cryptosystem RSA (without knowing the private key). What is the underlying hard mathematical problem for RSA? 2 p

   c) Explain in some detail which basic properties one wants from a public key cryptosystem? 4 p

2. a) Let a, b, m be positive integers. Give a criterion in terms of a, b, m for there to be a solution to the equation
$$ax \equiv b \mod m.$$
3 p

   b) Take a, b, m so that there is at least one solution to the equation,
$$ax \equiv b \mod m.$$
   Give an expression (in terms of a, b, m) for how many solutions there are modulo m. 3 p

   c) Use the Chinese reminder theorem to solve the following system of equations:
$$\begin{cases} 7x \equiv 3 \mod 10 \\ 7x \equiv 8 \mod 27 \end{cases}$$
2 p

3. a) Let G be a finite group and g an element of G. Prove how many multiplications that are needed, using fast powering, to compute g^N in terms of the positive integer N. Is the growth polynomial/subexponential/exponential with the input? 5 p

   b) Say that $p = 23$, $q = 564996057167345968 49$, $n = pq$ and that a is a primitive root both modulo p and modulo q. Roughly how many steps would it take for Pollard's $p-1$-algorithm, using the integer a as a base, to give the factorization of n? 3 p

4. a) State the ElGamal problem and state the Diffie-Hellman problem. 2 p

   b) Is the ElGamal problem easier to solve than the Diffie-Hellman problem? Is it harder? (No proof is necessary.) 1 p

   c) What are the algorithms involved in encryption and decryption in the ElGamal cryptosystem? What are their complexity? Are they polynomial/subexponential/exponential? 3 p

d) What is the fastest algorithm (that we know) that breaks the ElGamal cryptosystem? What is its complexity? Is it polynomial/subexponential/exponential? 2 p

5. a) Explain what a digital signature scheme is. 2 p

   b) What is the problem that digital signatures are supposed to solve? 2 p

   c) Explain the man-in-the-middle attack against a public key cryptosystem (of your choice). 2 p

   d) Does a digital signature protect against a man-in-the-middle attack? 2 p

6. a) Describe the Fermat primality test (that is, a primality test based upon Fermat's little theorem). 3 p

   b) What are the benefits of using the Miller-Rabin primality test compared to the Fermat primality test? 2 p

   c) What are the benefits of using the Fermat primality test compared to the Miller-Rabin primality test? 1 p

   d) What is the complexity of the Miller-Rabin primality test if one want to use it to get a primality proof? Is is polynomial/subexponential/exponential? 1 p

   e) Name an algorithm that gives a primality proof that has substantially better complexity than the Miller-Rabin primality test when used to give a primality proof. 1 p

7. a) What is a B-smooth number? 1 p

   b) Let p, q be prime numbers, $n = pq$, $a = \lfloor\sqrt{n}\rfloor + 1$, and $F(T) = T^2 - n$. Say that we have computed the list of integers $F(a), F(a+1), \ldots, F(a+b)$ for some positive integer b. Describe how the quadratic sieve gives all B-smooth numbers in this list (for any choice of positive integer B). 4 p

   c) Give an approximate expression for the number of divisions of integers one needs to do in the process described in b). 1 p

   d) Let n be of size 2^k. Give an expression for B that grows subexponentially with k, such that the expected number of checks of random integers of size roughly $\sqrt{n}$ one needs to do in order to find $\pi(B)$ integers that are B-smooth also grows subexponentially. What is this expected number? 2 p

8. a) Consider the elliptic curve over $\mathbb{F}_5$ given by,

$$E : y^2 = x^3 + 4x + 4.$$

   List the points of $E(\mathbb{F}_5)$. 2 p

   b) Lenstra's factorization algorithm is subexponential. Explain in some detail how this fact depends upon the distribution of B-smooth numbers. 6 p

9. Use index calculus to solve the DLP: $g^x \equiv_p h$ with $g = 103$, $h = 386$ and $p = 1019$. The fact that $hg^{183} = 126$ and the following table will be helpful:

$$\begin{pmatrix} i & g^i \pmod p \\ 946 & 2 \cdot 3 \cdot 5 \cdot 7 \\ 735 & 2 \cdot 3^2 \cdot 5 \\ 347 & 2^3 \cdot 3 \\ 245 & 3 \cdot 7 \\ 454 & 2 \cdot 3^2 \cdot 5 \cdot 7 \end{pmatrix}$$

8 p

10. a) What the expected number of steps for the Pollard-ρ method to find the solution to a DLP in $\mathbb{F}_p^*$? Is this algorithm polynomial/subexponential/exponential? 2 p

b) What is the main advantage of the Pollard-ρ method over Shank's Babystep-Giantstep method to solve a DLP? 1 p

c) The table

$$\begin{pmatrix} i & x_i & y_i & f(y_i) \\ 0 & 1 & 1 & 11 \\ 1 & 11 & 6 & 20 \\ 2 & 6 & 14 & 12 \\ 3 & 20 & 6 & 20 \\ 4 & 14 & 14 & \end{pmatrix}$$

describes an application of the function

$$f(x) = \begin{cases} gx \pmod p & \text{if } 0 \le x < 8 \\ x^2 \pmod p & \text{if } 8 \le x < 16 \\ hx \pmod p & \text{if } 16 \le x < 23 \end{cases}$$

where $p = 23$, $g = 11$, $h = 3$, $x_{i+1} = f(x_i)$ and $y_{i+1} = f(f(y_i))$. Use this data to solve the DLP: $g^x \equiv_p h$. 5 p

The exam will be returned 11.00 on Friday the 5th of April in room 410 in house 6. After that it can be collected in room 204 in house 6.