MATEMATISKA INSTITUTIONEN
STOCKHOLMS UNIVERSITET
Avd. Matematik
Examinator: Jonas Bergström

Tentamensskrivning i
Mathematics of Cryptography, 7,5 hp
24 April 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.

All answers must be motivated carefully! No calculators or computers may be used.

1. a) Explain how a public key cryptosystem and a private key cryptosystems works. 3 p

   b) What are the main advantages and disadvantages of using public key cryptosystems compared to private key cryptosystems. 3 p

   c) Give an example of how public key methods can be used together with a private key cryptosystem. 2 p

2. a) Give an example of a cryptosystem for which the underlying mathematical problem is assumed to be a DLP. 1 p

   b) Explain why it is a bad idea to base a cryptosystem on the DLP in the group $(\mathbb{Z}/n\mathbb{Z}, +)$. 2 p

   c) What is the main advantage of the DLP for elliptic curves compared to the DLP for $\mathbb{F}_p^*$? 2 p

   d) Explain a way to find a prime number p with 2040 bits, and give an expression for how many checks one is likely to have to do. 3 p

3. a) Let p be prime number and e be an integer. Give an expression (in terms of p, e) for how many solutions (modulo p) there are to the equation

$$x^e \equiv_p 1,$$

   and prove that it holds. 3 p

   b) The element $g = 7$ has order 23 in $\mathbb{F}_{47}^*$. Find all solutions (modulo 47) to the equation

$$7^{3x} \equiv_{47} 7.$$

   3 p

   c) Use the Chinese reminder theorem to solve the following system of equations:

$$\begin{cases} 3x \equiv 2 \mod 10 \\ 11x \equiv 8 \mod 27 \end{cases}$$

   2 p

4. a) Explain Shank's Babystep-Giantstep algorithm to solve DLPs in a finite group G. 3 p

   b) Prove that this algorithm always gives a solution. 2 p

   c) What is the complexity of Shank's Babystep-Giantstep algorithm and what is the complexity of the naive method to solve a DLP? Are they polynomial/subexponential/exponential? (No proofs are required.) 2 p

   d) What is the memory usage of Shank's Babystep-Giantstep algorithm and what is the memory usage of the naive method to solve the DLP? 1 p

5. a) Prove that the number of steps it takes, using the Euclidian algorithm, to find the greatest common divisor of two positive integers $a \geq b$ is at most $2\log_2(b) + 2$. 5 p

   b) Roughly how many steps does one need to solve the DLP $g^x = h$ in a finite group G using the naive method together with Pohlig-Hellman if g has order $5^{100} \cdot 7^{200}$? 3 p

6. a) Explain how the RSA cryptosystem works. 2 p

   b) Are there any type of integers $N = pq$ that should be avoided when setting up this cryptosystem? 1 p

   c) Explain how the RSA digital signature scheme works. 2 p

   d) Explain which purposes a hash function has when used in a digital signature scheme? 3 p

7. a) What is the difference between probabilistic encryption and deterministic encryption? 2 p

   b) Give an example of a cryptosystem with probabilistic encryption and one with deterministic encryption. 2 p

   c) Describe what kind of security problems there are with deterministic encryption. 2 p

   d) Describe what padding is and how it can turn a deterministic encryption into a probabilistic one. 2 p

8. a) Describe the index calculus algorithm to solve the DLP in $\mathbb{F}_p^*$. 3 p

   b) Give an expression for the complexity of the index calculus algorithm in terms of the prime p? Is it polynomial/subexponential/exponential? 2 p

   c) Explain how this complexity depends upon the distribution of smooth numbers (i.e. "how many" smooth numbers there are). 3 p

9. a) Consider the elliptic curve over $\mathbb{F}_7$ given by,

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

   List the points of $E(\mathbb{F}_7)$. 2 p

   b) The SEA-algorithm computes the number of points on an elliptic curve in polynomial time. Explain the importance of this algorithm for some cryptographical application. 2 p

   c) Explain in some detail what the main advantage of Lenstra's factorization algorithm is compared to Pollard's $p-1$-algorithm. 4 p

10. a) Let $N = 44377$, $F(T) = T^2 - N$ and $a = \lfloor\sqrt{N}\rfloor + 1 = 210$. Characterize which of the numbers:

$$F(a),\ F(a+1),\ F(a+2), \ldots, F(a+100)$$

that are divisible by 5 and which that are divisible by 11. 3 p

b) Now put $N = 3219577$, $F(T) = T^2 - N$ and $a = \lfloor\sqrt{N}\rfloor + 1 = 1794$. After computing $F(a+i)$ for i from 0 to 350 we find the following five 13-smooth numbers:

$$(a+7)^2 - N = 2^3 \cdot 3 \cdot 7 \cdot 11 \cdot 13, \quad (1)$$
$$(a+19)^2 - N = 2^6 \cdot 3^4 \cdot 13, \quad (2)$$
$$(a+59)^2 - N = 2^4 \cdot 3 \cdot 7^3 \cdot 13, \quad (3)$$
$$(a+73)^2 - N = 2^7 \cdot 3^3 \cdot 7 \cdot 11, \quad (4)$$
$$(a+227)^2 - N = 2^5 \cdot 3^3 \cdot 7 \cdot 11 \cdot 13, \quad (5)$$
$$(a+343)^2 - N = 2^3 \cdot 3^7 \cdot 7 \cdot 11. \quad (6)$$

Find all perfect squares one can form out of these numbers. 3 p

c) Write up all checks for factors of N coming from these perfect squares. You do not need to carry out the computations. 2 p

The exam will be returned 11.00 on Friday the 10th of May in room 410 in house 6. After that it can be collected in room 204 in house 6.