MATEMATISKA INSTITUTIONEN	Tentamensskrivning i
STOCKHOLMS UNIVERSITET	Mathematics of Cryptography, 7,5 hp
Avd. Matematik	25th April 2024
Examinator: Jonas Bergström	14.00-19.00

There are 8 problems with a total score of 80 points. The score from the exam is added to the score from the homework assignments. Grades are then given by the following intervals:

A 89-78p, B 77-69p, C 68-60p, D 59-51p, E 50-42p.

Remember to motivate your answers carefully. No calculators or computers may be used.

1. a) What is the main benefit/drawback of a symmetric cryptosystem compared to an asymmetric cryptosystem? 2 p

   b) What is the fastest method (we have seen in this course) to solve the DLP in an elliptic curve, and what is its complexity? 2 p

   c) Suppose an algorithm takes an input with k bits and requires $\mathcal{O}\left(e^{(\log k)^3}\right)$ steps to complete. Motivate if this algorithm runs in polynomial/subexponential/exponential time? 2 p

   d) Explain (briefly) how a digital signature scheme works. 2 p

   e) Explain (briefly) how the complexity of the index calculus depends upon the frequency of smooth integers. 2 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
$$ax \equiv_m b.$$
2 p

   b) Take positive integers a, b, m so that there is at least one solution to the equation,
$$ax \equiv_m b.$$
   Give an expression (in terms of a, b, m) for how many solutions there are modulo m. 2 p

   c) Show that if $\gcd(e, p-1) = 1$ then the equation
$$x^e \equiv_p a$$
   has a unique solution (modulo p) for all integers a. 3 p

   d) Describe the square-and-multiply algorithm when counting modulo an integer m. What is its complexity? 3 p

3. a) An elliptic curve E over $\mathbb{F}_{89}$ given by the equation $y^2 = x^3 + 59x + 1$ and $\#E(\mathbb{F}_{89}) = 75$. Let $P = (78, 35)$ and $Q = (14, 10)$ which are points in $E(\mathbb{F}_{89})$. Consider the DLP: $xP = Q$. Say that x_0 is a solution. Use the following table to determine x_0 modulo 5.
$$\begin{pmatrix} i & 3 & 5 & 6 & 9 & 15 & 25 & 30 \\ iP & (81,68) & (7,57) & (0,1) & (10,16) & (59,44) & (77,18) & (60,45) \\ iQ & (73,52) & (22,33) & (71,82) & (81,68) & (60,45) & (77,71) & (59,45) \end{pmatrix}$$
3 p

b) Describe which computations (without carrying them out) one would need to make to continue the Pohlig-Hellman algorithm to solve the DLP above. 4 p

c) Give an expression for the complexity of Shank's baby-step giant-leap method combined with the Pohlig-Hellman algorithm to solve the DLP in a group with N elements. 3 p

4. a) Describe how the RSA cryptosystem works. 3 p

b) What is the RSA-problem? 1 p

c) The version of RSA that is described in the book is deterministic. It is therefore not considered to be safe to use in practice. Describe a situation when this weakness could be effectively exploited. 2 p

d) Describe (including some details) what padding is and how it can turn a deterministic encryption into a probabilistic one. 3 p

e) What is the main drawback of adding padding to the encryption? 1 p

5. a) Describe the Fermat primality test. 2 p

b) What is a Carmichael number? 1 p

c) Say that n is a composite number that is not a Carmichael number. Show that at least half of all integers between 2 and $n-1$ are Fermat witnesses of compositeness. 3 p

d) Is there a Miller-Rabin witness for each composite number n? 1 p

e) Give an expression, with a motivation, for how many random integers with k digits one would expect to check to find a prime number. 3 p

6. 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:

$$\begin{aligned}
(a+7)^2 - N &= 2^3 \cdot 3 \cdot 7 \cdot 11 \cdot 13,\\
(a+19)^2 - N &= 2^6 \cdot 3^4 \cdot 13,\\
(a+59)^2 - N &= 2^4 \cdot 3 \cdot 7^3 \cdot 13,\\
(a+73)^2 - N &= 2^7 \cdot 3^3 \cdot 7 \cdot 11,\\
(a+227)^2 - N &= 2^5 \cdot 3^3 \cdot 7 \cdot 11 \cdot 13,\\
(a+343)^2 - N &= 2^3 \cdot 3^7 \cdot 7 \cdot 11.
\end{aligned}$$

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

d) Give an expression for the complexity of this algorithm (the quadratic sieve together with factorization via difference of squares). State also if the algorithm runs in polynomial/ subexponential/exponential time. 2 p

7. Say that you want to set up ECDH (elliptic curve Diffie-Hellman key exchange).

a) Say that we can generate a large prime p. Are there any types of primes that one should avoid? 1 p

b) Describe how to (in an efficient/fast way) find an elliptic curve E defined over $\mathbb{F}_p$. 2 p

c) Are there any types of elliptic curves that one should avoid? 2 p

d) What property do we want from a point P in $E(\mathbb{F}_p)$ to make ECDH secure? 1 p

e) Describe the algorithms involved with their complexity, to efficiently/fast find a point P with this property. 4 p

8. a) Describe Lenstra's elliptic curve method to factor integers. 4 p

b) Is this algorithm exponential/subexponential/polynomial? 1 p

c) Given an integer N, how can one in an efficient way find two integers a, b such that $4a^3 + 27b^2 \not\equiv_N 0$ together with a solution $(x, y) = (x_0, y_0)$ to the equation $y^2 \equiv_N x^3 + ax + b$? 1 p

d) Explain why Lenstra's factorization method (in general) is faster than Pollard's $p - 1$ even though they are based on the same idea. 4 p