MATEMATISKA INSTITUTIONEN
STOCKHOLMS UNIVERSITET
Avd. Matematik
Examinator: Jonas Bergström

Tentamensskrivning i
Mathematics of Cryptography, 7,5 hp
8th May 2026
08.00-13.00

There are 7 problems with a total score of 70 points. The score from the exam is added to the score from the homework assignments. Grades will be given by the following intervals:

A 76-67p, B 66-59p, C 58-51p, D 50-43p, E 42-35p.

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

1. a) Explain in what situations an asymmetric cryptosystem is preferable to a symmetric key cryptosystem and why? 2 p

   b) What is a pseudorandom number generator and how can they be used in symmetric cryptosystems? 2 p

   c) Using the prime number theorem, what is the expected number of integers with k digits one needs to check to find one that is prime? 2 p

   d) For what types of integers is Pollard's $p-1$ algorithm for factoring integers efficient? 1 p

   e) What does Hasse's theorem say about the number of points of an elliptic curve defined over a finite field $\mathbb{F}_p$? 2 p

   f) What is the advantage that cryptosystems based on the shortest vector problem in a lattice is believed to have compared to cryptosystems based on the ECDLP? 1 p

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

   b) Say that $p \equiv_4 3$. Fix any $a \not\equiv_p 0$. Show that if the equation $x^2 \equiv_p a$ has a solution, then its solutions are $a^{(p+1)/4}$ and $-a^{(p+1)/4}$. Show furthermore that if the equation $x^2 \equiv_p a$ does not have a solution then $a^{(p+1)/2} \equiv_p -a$. 3 p

   c) Say that p, q are distinct primes, $n = pq$ and that a is an integer, for which $\gcd(a, pq) = 1$. Say that a has order k in $\mathbb{F}_p^*$. Say that a has order l in $\mathbb{F}_q^*$. Show that a has order $\mathrm{lcm}(k, l)$ in $(\mathbb{Z}/n)^*$, where $\mathrm{lcm}(k, l)$ denotes the least common multiple of k and l, 4 p

3. a) State the collision theorem, that is, what is the probability that you have after making m random choices of balls from an urn (containing n red and $N-n$ blue balls) have gotten at least one red ball. 1 p

   b) If we assume that $n \approx m$, then roughly how many balls do you need to pick in order to expect to get a red ball? 1 p

   c) Using the collision theorem, explain the expected running time of the probabilistic version of Shank's babystep-giantstep algorithm. 4 p

   d) Describe Pollard's ρ-method for solving the ECDLP (the elliptic curve discrete logarithm problem), and how its expected running time is connected to the collision theorem. 4 p

4. Let $N = 1769461$, $F(T) = T^2 - N$ and $a = \lfloor \sqrt{N} \rfloor + 1 = 1330$. After computing $F(a+i)$ for i from 0 to 6000 we find the following seven 11-smooth numbers:

$$\begin{aligned}
(a+1)^2 - N &= 2^2 \cdot 3 \cdot 5^2 \cdot 7, \\
(a+6)^2 - N &= 3^2 \cdot 5 \cdot 7^3, \\
(a+286)^2 - N &= 3^7 \cdot 5 \cdot 7 \cdot 11, \\
(a+421)^2 - N &= 2^2 \cdot 3^3 \cdot 5 \cdot 7^4, \\
(a+3289)^2 - N &= 2^2 \cdot 3 \cdot 5^2 \cdot 7^2 \cdot 11^3, \\
(a+4389)^2 - N &= 2^2 \cdot 3^2 \cdot 5^7 \cdot 11, \\
(a+5951)^2 - N &= 2^2 \cdot 5^3 \cdot 7 \cdot 11^4.
\end{aligned}$$

   a) Characterize which of the numbers of the form $F(a+i)$ above that are divisible by 13. 2 p

   b) Write the matrix equation for finding the perfect squares that one can form out of the seven 11-smooth numbers. 3 p

   c) Compute all perfect squares that one can form out of the seven 11-smooth numbers. 3 p

   d) Explain how one can use a perfect square from the former step to check for factors of N (no computation is necessary). 2 p

5. a) Explain the index calculus for solving the DLP in $\mathbb{F}_p^*$. 6 p

   b) Give a rough explanation for the complexity of the index calculus. 3 p

   c) Is the complexity exponential/subexponential/polynomial? 1 p

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

   a) Explain briefly how one can generate a large prime p. 2 p

   b) Describe how to find an elliptic curve E defined over $\mathbb{F}_p$. 1 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 briefly how one can find such an elliptic curve and point. 2 p

   f) Explain how the ECDH works. 2 p

7. a) Define what a basis of a lattice $L \subset \mathbb{R}^n$ is. 1 p

   b) How are different bases of a lattice $L \subset \mathbb{R}^n$ related? 1 p

   c) Explain what the Hadamard ratio is and how it measures the orthogonality of a basis of a lattice. 3 p

   d) What is the private key and the public key in the GGH cryptosystem? 3 p

   e) Explain how to solve the SVP (shortest vector problem) in a lattice $L \subset \mathbb{R}^n$ of dimension n, if you have an orthogonal basis of L. 2 p