MATEMATISKA INSTITUTIONEN
STOCKHOLMS UNIVERSITET
Avd. Matematik
Examinator: Jonas Bergström

Tentamensskrivning i
Mathematics of Cryptography, 7,5 hp
21st March 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 what a symmetric cryptosystem and an asymmetric cryptosystem is, and explain their main differences. 2 p

   b) What does Kerkhoff's principle say? 1 p

   c) What is the fastest algorithm that solves the ECDLP (the elliptic curve discrete logarithm problem) and is its complexity polynomial/subexponential/exponential? 2 p

   d) Explain why it is not considered secure to use deterministic encryption. 2 p

   e) Explain Shank's babystep-giantstep algorithm to solve a DLP in a finite group. 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) Say that G is a group with $N = p_1^{r_1} \cdot \ldots \cdot p_k^{r_k}$ elements and where $p_1, \ldots, p_k$ are distinct primes. Show that one can find the order an element $g \in G$ by computing g^k for at most $-1 + (r_1 + 1)(r_2 + 1) \cdots (r_k + 1)$ values of k. 2 p

   b) 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

   c) Say that p is prime. Let e, c be integers where p does not divide c. Put $d = \gcd(e, p - 1)$. Show that the equation $x^e \equiv_p c$ has a solution if and only if $c^{(p-1)/d} \equiv_p 1$. 4 p

3. a) Describe the problem a digital signature scheme is supposed to solve. 1 p

   b) Explain the principles of how a digital signature scheme works. 4 p

   c) Explain why a hash function is typically used in a digital signature scheme. 2 p

   d) Describe the meddler-in-the-middle attack. 2 p

   e) Explain why digital signature schemes do not completely solve the issue of meddler-in-the-middle attacks? 1 p

4. For a prime p, define the function $f : \{0, 1, \ldots, p-1\} \to \{0, 1, \ldots, p-1\}$ by

$$f(x) = \begin{cases} gx \mod p & \text{if } x = 1 \mod 3 \\ x^2 \mod p & \text{if } x = 2 \mod 3 \\ hx \mod p & \text{if } x = 0 \mod 3. \end{cases}$$

We use the Pollard-ρ algorithm with the function f and $p = 47$ applied to the DLP:

$$5^x = 15 \mod 47.$$

Putting $x_1 = y_1 = 1$ and $x_{i+1} = f(x_i)$ and $y_{i+1} = f(f(y_i))$ we get the following table,

i	$x_i \mod 3$	$y_i \mod 3$	$f(y_i) \mod 3$
1	1	1	2
2	2	1	1
3	1	2	2
4	1	2	1
5	2	2	0
6	2	0	2
7	2	1	2
8	1	0	0
9	2	2	1

with $x_{10} = 3$ and $y_{10} = 35$. Continue the Pollard-ρ algorithm to solve the DLP above. 10 p

5. a) Explain, with some details, how the three different steps: relation building, elimination and gcd-computation, works in the difference of squares method, together with the quadratic sieve, for factoring integers. 5 p

   b) What is the assumption that one makes in order to determine the complexity of this algorithm? 2 p

   c) Explain briefly how the distribution of B-smooth numbers determines the complexity of the algorithm. 2 p

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

6. a) Explain how to generate a large (probable) prime p and the algorithms involved. 3 p

   b) Given the large prime p, explain how to find an elliptic curve $E(\mathbb{F}_p)$ together with a point $P \in E(\mathbb{F}_p)$ to set up a secure instance of an elliptic curve Diffie-Hellman key exchange. 5 p

   c) Let E be the elliptic curve over $\mathbb{F}_7$ given by the Weierstrass equation $y^2 = x^3 + x + 1$ and let $P = (0, 1) \in E(\mathbb{F}_7)$. Compute $-3P$. 2 p

7. a) Let $L \subset \mathbb{R}^n$ be a lattice of dimension n. Let V be a basis of L. Define what a fundamental domain $\mathcal{F}(V)$ for L corresponding to V is, and prove that any vector in $\mathbb{R}^n$ can be written uniquely as a sum of a vector in L and a vector in $\mathcal{F}(V)$. 3 p

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

   c) Explain how the NTRU Key Recovery Problem can be reformulated as a lattice SVP. 3 p

   d) Explain why ternary polynomials are used in NTRUEncrypt. 2 p