MATEMATISKA INSTITUTIONEN
STOCKHOLMS UNIVERSITET
Avd. Matematik
Examinator: Jonas Bergström

Tentamensskrivning i
Mathematics of Cryptography, 7,5 hp
18th March 2025
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 $\mathbb{F}_p^*$, and what is its complexity? 1 p

   c) Name the mathematical problems that we have seen in this course (and on which we have based cryptographic algorithms) that can be solved fast (in polynomial time) on a *quantum* computer? 1 p

   d) For which choices of integers $N = pq$, with p, q primes, is Pollard's $p-1$ factorization algorithm fast? 1 p

   e) Explain how a Fermat primality test works. 2 p

   f) Explain how the LLL-algorithm together with Babai's algorithm can be used to solve the apprCVP. 3 p

2. a) Show that the Euclidean algorithm runs in polynomial time. 3 p

   b) Let p, q be two distinct primes. Show that the equation $x^e \equiv_{pq} 1$ has a unique solution if and only if $\gcd(e, (p-1)(q-1)) = 1$. 3 p

   c) Show that the Weierstrass equation $y^2 = x^3 + 2x + 4$ over the field $\mathbb{F}_{17}$ defines an elliptic curve $E(\mathbb{F}_p)$. 1 p

   d) Show that $P = (0, 2)$ and $Q = (13, 0)$ are elements of $E(\mathbb{F}_{17})$. 1 p

   e) Compute $2P$, $4P$ and $P + Q$ in $E(\mathbb{F}_{17})$. 2 p

3. Solve the DLP $xP = Q$ where $P = (78, 35)$ and $Q = (14, 10)$ are points on the elliptic curve E over $\mathbb{F}_{89}$ given by the equation $y^2 = x^3 + 59x + 1$ and which has 75 points all together. Use the Pohlig-Hellman algorithm, the fact that $(73, 52) = (60, 44) + (0, 1)$, and the following table:

$$\begin{pmatrix} i & 3 & 5 & 6 & 9 & 15 & 25 & 30 \\ iP & (81,68) & (7,57) & (0,1) & (10,16) & (59,44) & (77,18) & (60,45) \\ iQ & (73,52) & (22,33) & (71,82) & (81,68) & (60,45) & (77,71) & (59,45) \end{pmatrix}.$$

10 p

4. a) Describe how the RSA digital signature scheme works. 3 p

   b) What is the meddler-in-the-middle attack? 1 p

   c) Explain why a digital signature scheme protects, or why it does not protect, against a meddler-in-the-middle attack? 2 p

   d) Explain what a hash function is. 1 p

   e) Explain how a hash function often is used together with digital signature schemes? 1 p

   f) Explain why a hash function often is used together with digital signature schemes? 2 p

5. a) Explain in detail how the three different steps: relation building, elimination and gcd-computation, works in the quadratic sieve algorithm (together with the difference of squares) for factoring integers. 6 p

   b) Explain how the complexity of the relation building step depends on the distribution of B-smooth numbers. 3 p

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

6. a) State the collision theorem. 1 p

   b) Give an abstract formulation of Pollard's ρ algorithm. 2 p

   c) What is the expected running time for Pollard's ρ algorithm? 1 p

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

   e) Explain how the expected running time for Pollards ρ algorithm connects to the collision theorem. 3 p

   f) Explain how one can one use Pollard's ρ algorithm to solve a DLP? 2 p

7. ECDSA is set up with a prime p, an elliptic curve $E(\mathbb{F}_p)$ and a point $G \in E(\mathbb{F}_p)$ of prime order q. Samantha chooses a secret signing key $1 \leq s \leq q-1$, computes $V = sG$, and publishes the verification key V. Samantha then chooses a document $1 \leq d \leq p$, and a random element $1 < e < q$. Samantha then computes the signature $s_1 \equiv_q x(eG)$ and $s_2 \equiv_q e^{-1}(d + s \cdot s_1)$. Finally Samantha sends $(d, (s_1, s_2))$ to Victor. Victor then computes $v_1 \equiv_q ds_2^{-1}$, $v_2 \equiv_q s_1 s_2^{-1}$.

   a) Show that if Samantha has signed the document then $x(v_1 G + v_2 V)$ is equal to $s_1 \bmod q$. 2 p

   b) Say that Samantha signs documents d and d' using the same random element e. Show how that can be used to find Samantha's secret signing key s. 2 p

   c) In setting up the ECDSA, describe the algorithms involved to find the large prime p. 2 p

   d) Describe how to then find an elliptic curve $E(\mathbb{F}_p)$ and a point $G \in E(\mathbb{F}_p)$ of prime order q, where q has roughly the same size as p. 3 p

   e) Are there any types of elliptic curves that one should avoid? 1 p

8. a) Compute the inverse of $x^4 + 1$ in $\mathbb{F}_{11}[x]/(x^5 - 1)$. 3 p

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

   c) State the NTRU Key Recovery Problem. 1 p

   d) Roughly how many steps does the brute force method take to solve the NTRU Key Recovery Problem? 1 p

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