MATEMATISKA INSTITUTIONEN
STOCKHOLMS UNIVERSITET
Avd. Matematik
Examinator: Jonas Bergström

Tentamensskrivning i
Mathematics of Cryptography, 7,5 hp
15th March 2024
08.00-13.00

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 do we mean by a one-way-function with a trapdoor? 2 p

   b) Define the terms symmetric cryptosystem and asymmetric cryptosystem and explain their main differences. 2 p

   c) Define what it means for an algorithm to be subexponential. 2 p

   d) What types of elliptic curves should one avoid if one wants to use them in the Elliptic curve Diffie-Hellman key exchange? 2 p

   e) Describe how the ECIES (Elliptic Curve Integrated Encryption Scheme) includes both symmetric and asymmetric algorithms. 2 p

2. a) Use the Chinese remainder theorem to find all integer solutions to the following system of equations:

$$\begin{cases} 3x \equiv 5 \mod 7 \\ 3x \equiv 21 \mod 22 \\ 7x \equiv 19 \mod 27. \end{cases}$$

   3 p

   b) Say that $N = p_1^{r_1} \cdot \ldots \cdot p_k^{r_k}$ where $p_1, \ldots, p_k$ are distinct primes and that G is a group with N elements. Show that an element $g \in G$ is a generator of G if and only if $g^{N/p_i} \neq 1$ for all $i = 1, \ldots, k$. 4 p

   c) 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

3. a) Describe the Diffie-Hellman key exchange in an arbitrary group. 3 p

   b) Which types of public parameters for the Diffie-Hellman key exchange in $\mathbb{F}_p^*$ should one avoid? 2 p

   c) Describe how (i.e. the algorithms involved and the expected number of operations of these) to find (good) public parameters for the Diffie-Hellman key exchange in $\mathbb{F}_p^*$. 5 p

4. a) Describe the problem a digital signature scheme is supposed to solve. 2 p

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

   c) Describe the Elliptic curve digital signature scheme. 4 p

   d) Explain why digital signature schemes do not completely solve the issue of meddler-in-the-middle attacks? 2 p

5. a) What is the complexity of the index calculus? 2 p

   b) Use index calculus to solve the DLP in $\mathbb{F}_{167}^*$:

$$17^x \equiv 77 \mod 167.$$

   The fact that $77 \cdot 17^{-140} = 108$ and the following table will be helpful:

$$\begin{pmatrix} i & 17^i \mod 167 \\ 34 & 72 \\ 37 & 30 \\ 53 & 112 \\ 139 & 90 \end{pmatrix}$$

   8 p

6. a) Explain in detail 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. 6 p

   b) Explain how the choice of the smoothness bound B affects the complexity. 3 p

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

7. a) Let P be a point on an elliptic curve E defined over a finite field $\mathbb{F}_p$. Use Hasse's theorem to give an upper bound for the order of P. 2 p

   b) For which primes p does the Weierstrass equation $y^2 = x^3 + 2x + 4$ define an elliptic curve over $\mathbb{F}_p$? 2 p

   c) Consider the elliptic curve

$$E : y^2 = x^3 + 2x + 4$$

   defined over $\mathbb{F}_{17}$ and the points $P = (0, 2)$ and $Q = (13, 0)$. Compute $2P, 4P$ and $P + Q$. 3 p

   d) Explain why Lenstra's factorization algorithm (in general) is faster than Pollard's $p - 1$ factorization algorithm even though they are based on the same idea. 3 p

8. a) Let p be a prime and $E(\mathbb{F}_p)$ be an elliptic curve given by the Weierstrass equation $y^2 = x^3 + ax + b$. Let P and Q be points in $E(\mathbb{F}_p)$, and assume that $\#E(\mathbb{F}_p)$ is known. Consider the DLP: $xP = Q$. Define the function $f : E(\mathbb{F}_p) \to E(\mathbb{F}_p)$ by

$$f(R) = \begin{cases} R + P - Q & \text{if } R = \mathcal{O} \text{ or } R_x = 0 \mod 3 \\ R + 2P + Q & \text{if } R_x = 1 \mod 3 \\ R + P + 3Q & \text{if } R_x = 2 \mod 3 \end{cases}$$

for any point $R = (R_x, R_y)$ on $E(\mathbb{F}_p)$ with $0 \leq R_x < p$. Put $X_0 = Y_0 = \mathcal{O}$, $X_{i+1} = f(X_i)$ and $Y_{i+1} = f(f(Y_i))$. Say that after computing N values of X_i and Y_i you find that $X_N = Y_N$. Explain how this information can be used to solve the DLP? 4 p

b) We expect N in general to be of size $\sqrt{p}$. Explain why. 4 p

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

d) What is the complexity of the fastest known algorithm to compute $\#E(\mathbb{F}_p)$? 1 p