MATEMATISKA INSTITUTIONEN
STOCKHOLMS UNIVERSITET
Avd. Matematik
Examinator: Jonas Bergström
Lecturer: Tuomas Tajakka

Tentamensskrivning i
Mathematics of Cryptography, 7,5 hp
14 March 2023
14.00-19.00

There are 2 pages and 8 problems with total score of 85 points. The score from the exam is added to the score from the homework assignments. Grades are then given by the following intervals:

A: 100-92 p   B: 91-84 p   C: 83-76p   D: 75-68 p   E: 67-60 p

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

1. Define the following terms:

   a) symmetric key cryptosystem — 2 p

   b) chosen plaintext attack — 2 p

   c) cryptographic hash function — 2 p

   d) encoding scheme — 2 p

   e) big-$\mathcal{O}$ notation — 3 p

2. a) State Fermat's little theorem. — 2 p

   b) Use Fermat's little theorem and the fast powering algorithm to find the multiplicative inverse of 5 in $\mathbb{F}_{13}$. Show all steps. — 4 p

   c) In general, how many multiplications does the fast powering algorithm require? — 4 p

3. a) What do we mean by the discrete logarithm problem in a finite group G? — 2 p

   b) Consider the following invertible matrices with coefficients in $\mathbb{F}_7$:

$$g = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \quad h = \begin{pmatrix} 1 & 0 \\ 6 & 1 \end{pmatrix}.$$

   Implement Shank's algorithm to solve the DLP $g^x = h$. You might find useful the identity

$$g^7 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

   4 p

   c) What is the running time of Shank's algorithm for solving the DLP in $\mathbb{F}_p^*$? Explain. — 4 p

4. a) Describe the Pohlig-Hellman algorithm. — 4 p

   b) Using a cryptosystem based on the DLP in $\mathbb{F}_p^*$, how should you choose the modulus p in order to shield against the Pohlig-Hellman algorithm? — 2 p

   c) What is the running time of the Pohlig-Hellman algorithm together with the naive algorithm to solve a DLP in a group with N elements? — 3 p

5. a) Describe the RSA public key cryptosystem and explain what role Euler's theorem plays in it. 3 p

   b) Solve the congruence:
$$x^{27} \equiv 52 \mod 55$$
4 p

   c) Alice and Bob both create keys for the RSA cryptosystem. They both choose the modulus $N = 8549$, but Alice's encryption key is $e_A = 5$ while Bob's is $e_B = 4187$. Eve encrypts the message $m = 44$ using both keys and finds that the ciphertexts coincide. Using this information help Eve factor the modulus N. (*Hint:* $93^2 = 8649$.) 5 p

6. a) Let $N = 44377$, $F(T) = T^2 - N$, and $a = \lfloor\sqrt{N}\rfloor + 1 = 210$. Characterize which of the numbers
$$F(a), F(a+1), F(a+2), \ldots, F(a+100)$$
are divisible by 5 and which are divisible by 11. 3 p

   b) Now set $N = 3219577$, $F(T) = T^2 - N$, and $a = \lfloor\sqrt{N}\rfloor + 1 = 1794$. After computing $F(a+i)$ for $i = 0, \ldots, 350$, we found the following 13-smooth numbers:
$$(a+7)^2 - N = 2^3 \cdot 3 \cdot 7 \cdot 11 \cdot 13$$
$$(a+19)^2 - N = 2^6 \cdot 3^4 \cdot 13$$
$$(a+59)^2 - N = 2^4 \cdot 3 \cdot 7^3 \cdot 13$$
$$(a+73)^2 - N = 2^7 \cdot 3^3 \cdot 7 \cdot 11$$
$$(a+227)^2 - N = 2^5 \cdot 3^3 \cdot 7 \cdot 11 \cdot 13$$
$$(a+343)^2 - N = 2^3 \cdot 3^7 \cdot 7 \cdot 11$$

   Find at least four perfect squares one can form out of these numbers. 4 p

   c) Write down all the checks for factors of N coming from the perfect squares you found in (b). You do not need to carry out the computations. 4 p

7. a) Consider the elliptic curve $E : y^2 = x^3 + x + 1$ over $\mathbb{F}_5$. Check that E indeed is an elliptic curve and that the points $P = (2, 4)$ and $Q = (3, 1)$ are on E, and calculate $P + Q$. 3 p

   b) An *inflection point* of an elliptic curve E is a point P where the tangent line meets E with multiplicity 3. What is the order of such at point P? Draw a picture. 3 p

   c) Let E be an elliptic curve over $\mathbb{F}_{53}$. Explain why the number of points on E is between 39 and 69. 3 p

   d) Why is the fast powering algorithm particularly fast on an elliptic curve compared to an arbitrary group? 1 p

8. a) Describe the elliptic curve Diffie-Hellman key exchange. How should the public parameters be chosen? 4 p

   b) What is the main benefit of cryptosystems based on elliptic curves compared to those based on $\mathbb{F}_p^*$? 3 p

   c) Describe Lenstra's factorization algorithm. What kinds of numbers does it factor particularly efficiently? 5 p