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

Tentamensskrivning i
Mathematics of Cryptography, 7,5 hp
18 March 2022
14.00-19.00

There are 3 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. a) Use the fast powering algorithm to compute $3^{41} \bmod 7$. 4 p

   b) Solve the following system of congruences:

$$\begin{cases} 2x & \equiv 1 \mod 5 \\ x & \equiv 2 \mod 8 \\ x-1 & \equiv 4 \mod 7 \end{cases}$$

   4 p

   c) List all units in the ring $\mathbb{Z}/20$. 2 p

2. Certain individuals decide to use the RSA public key cryptosystem to communicate.

   a) Agnetha secretly chooses primes p and q and publishes the modulus $N = pq$ and an encryption key e. She receives the cipher text c from Björn. How did Björn obtain c, and what calculations does Agnetha have to perform to recover Björn's message? Explain why her calculations work. 5 p

   b) Agnetha wrote down the value of $M = (p-1)(q-1)$ on a piece of paper to aid her computations. However, Eavesdropper Elton finds this paper. Explain how Elton can combine this new knowledge with publicly available information to discover the secret primes p and q. 2 p

   c) Anni-Frid and Benny also wants to communicate, so Anni-Frid creates RSA keys and broadcasts the public key to Benny. However, Elton has managed to take over the entire communication channel the two are using. Explain how Elton can launch a meddler-in-the-middle attack against them. 3 p

3. a) Describe the Miller-Rabin primality test. 4 p

   b) What is the complexity of the Miller-Rabin test in terms of the number of binary digits of the integer n to be tested? 3 p

   c) After some preliminary experiments, Alice suspects that a large integer n is a prime. She wants to gain more evidence for this using the Miller-Rabin test. Given a percentage $0 < p < 100$, write down a formula for how many values a she should check to be p % sure? 4 p

   d) What is the main benefit of the Miller-Rabin primality test over the Fermat primality test? Why is the Fermat test nevertheless useful? 2 p

4. a) Describe Shank's baby-step giant-step algorithm for solving the discrete logarithm problem $g^x = h$ in a group G. 3 p

   b) Show that Shank's algorithm is guaranteed to find a solution, provided one exists. 3 p

   c) Let p be a prime number and suppose that $p-1 = q_1q_2q_3$ is the product of 3 distinct primes. Consider the discrete logarithm problem $g^x = h$ where $g \in \mathbb{F}_p^*$ is a primitive root. Explain how the Chinese Remainder Theorem can be used to help find a solution. 3 p

   d) What is the main benefit of Pollard's ρ method compared to Shank's algorithm? 1 p

5. a) Describe the ElGamal public key cryptosystem. 3 p

   b) What is the purpose of a digital signature scheme? 3 p

   c) List some of the properties required from a cryptographic hash function. 2 p

6. Suppose we wish to factor the RSA modulus $N = pq$ using the quadratic sieve method.

   a) The first step is to choose a "smoothness parameter" B. What is the drawback of choosing B too small compared to N? What about too large? 3 p

   b) Suppose that $N = 1569929$. Define the function $F(T) = T^2 - N$ and consider the values

   $$F(2491),\ F(2492),\ F(2493),\ F(2494),\ \ldots,$$

   Which values on the list are divisible by the prime $p = 5$? Explain. 5 p

   c) Suppose that $N = 1569929$ and $B = 19$. Quadratic sieving yields the following table:

   $$\begin{pmatrix} a & a^2 \bmod N \\ 1253 & 2^4 \cdot 5 \\ 1255 & 2^3 \cdot 7^2 \cdot 13 \\ 1258 & 5 \cdot 7 \cdot 19^2 \\ 1267 & 2^5 \cdot 5 \cdot 13 \cdot 17 \\ 1269 & 2^4 \cdot 7 \cdot 19^2 \\ 1277 & 2^7 \cdot 5^2 \cdot 19 \\ 1283 & 2^7 \cdot 5 \cdot 7 \cdot 17 \\ 1293 & 2^5 \cdot 5 \cdot 7^2 \cdot 13 \end{pmatrix}$$

   Write down a matrix equation over the field $\mathbb{Z}/2$ that can be used to find solutions to the equation $x^2 \equiv y^2 \mod 1569929$. 4 p

7. Consider the equation $y^2 = x^3 + 1$ over $\mathbb{F}_7$.

   a) Check that $y^2 = x^3 + 1$ actually defines an elliptic curve E over $\mathbb{F}_7$. 2 p

   b) Show that $P = (0, 1)$ and $Q = (6, 0)$ are points on E, and compute $3P$, $2Q$ and $P + Q$. 4 p

   c) Count the number of points of E over $\mathbb{F}_7$. 3 p

   d) Is $E(\mathbb{F}_7)$ a cyclic group? 3 p

8. Let E be an elliptic curve over $\mathbb{F}_p$ with p a prime number.

   a) What does the Hasse bound tell us about how many points $E(\mathbb{F}_p)$ can have? 2 p

b) One application of elliptic curves in cryptography is the elliptic ElGamal cryptosystem. Explain why it is not obvious how to encode messages when using the elliptic ElGamal cryptosystem. 1 p

c) Suppose that the public parameters are given for elliptic curve Diffie-Hellman key exchange. What are the algorithms involved in making the actual key exchange and what are their complexities? 3 p

d) Describe Lenstra's factorization algorithm. Explain in particular 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. 4 p