TECHNISCHE UNIVERSITEIT EINDHOVEN
Faculty of Mathematics and Computer Science
Exam Cryptography 1, Tuesday 14 April 2015

Name :

TU/e student number :

Exercise	1	2	3	4	5	total
points						

Notes: Please hand in this sheet at the end of the exam. You may keep the sheet with the exercises.
This exam consists of 5 exercises. You have from 13:30 – 16:30 to solve them. You can reach 100 points.
Make sure to justify your answers in detail and to give clear arguments. Document all steps, in particular of algorithms; it is not sufficient to state the correct result without the explanation. If the problem requires usage of a particular algorithm other solutions will not be accepted even if they give the correct result.
All answers must be submitted on TU/e letterhead; should you require more sheets ask the proctor. State your name on every sheet.
Do not write in red or with a pencil.
You are allowed to use any books and notes, e.g. your homework. You are not allowed to use the textbooks of your colleagues.
You are allowed to use a calculator without networking abilities. Usage of laptops and cell phones is forbidden. One laptop is available at the front of the room to look up things from the course web pages, the course scripts, or do calculations with GP-Pari.

1. This problem is about the DH key exchange. The public parameters are that the group is $(\mathbb{F}_{1013}^*, \cdot)$ and that it is generated by $g = 7$.

   (a) Compute the public key belonging to the secret key $b = 580$.

   2 points

   (b) Alice's public key is $h_a = 848$. Compute the shared DH key with Alice using b from the previous part.

   4 points

2. This exercise is about computing discrete logarithms in some groups.

   (a) Alice and Bob use $(\mathbb{Z}/34567, +)$ for Diffie-Hellman with generator $g = 7$. You observe that Alice uses $h_a = a \cdot g = 12345$ and Bob uses $h_b = b \cdot g = 23456$. Compute the shared Diffie-Hellman key of Alice and Bob. 3 points

   (b) The order of 19 in $(\mathbb{F}_{337}^*, \cdot)$ is 336. Charlie uses the group generated by $g = 19$ for cryptography. His public key is $g_c = 123$. Use the Pohlig-Hellman attack to compute the discrete logarithm of g_c to the base g. 20 points

3. This exercise is about factoring $n = 4891$.

   (a) Use Pollard's rho method of factorization to find a factor of 4891. Use starting point $x_0 = 3$, iteration function $x_{i+1} = x_i^2 + 1$ and Floyd's cycle finding method, i.e. compute $\gcd(x_{2i} - x_i, 4891)$ until a non-trivial gcd is found.

   8 points

   (b) Perform one round of the Fermat test with base $a = 2$ to test whether 4891 is prime. What is the answer of the Fermat test?

   5 points

   (c) Use Pollard's $p - 1$ factorization method to factor the number $m = 4891$ with base $u = 8$ and exponent $s = \mathrm{lcm}(\{1, 2, 3, 4\})$.

   5 points

4. (a) Find all affine points on the Edwards curve $x^2 + y^2 = 1 - 6x^2y^2$ over $\mathbb{F}_{17}$.

   10 points

   (b) Verify that $P = (3, 10)$ is on the curve.

   1 point

   (c) Compute $5P$.

   11 points

   (d) Translate the curve and P to Montgomery form

$$Bv^2 = u^3 + Au^2 + u.$$

   5 points

5. This exercise is about the NTRU encryption system. The system has three general public parameters: namely positive integers N, p, and q, where $\gcd(p, q) = 1$ and q is much larger than p. For this exercise we use $p = 3, q = 101$, and $N = 7$.

   All computations take place in $R = \mathbb{Z}[x]/(x^N - 1)$, i.e. all elements are represented by polynomials of degree $< N$. Some computations additionally reduce modulo p or modulo q.

   The private key of user Alice is a polynomial $f(x) \in R$ which satisfies that f is invertible in $R/p = (\mathbb{Z}/p)[x]/(x^N - 1)$ and in $R/q = (\mathbb{Z}/q)[x]/(x^N - 1)$.

   To generate her public key, Alice picks a polynomial $g(x) \in R$ and computes $f_p = f^{-1}$ in R/p, $f_q = f^{-1}$ in R/q and $h = f_q \cdot g$ in R/q. Alice's public key is h along with the public paramters p, q, and N.

   To encrypt message $m(x) \in R$ (with coefficients in $[-(p-1)/2, (p-1)/2]$) to a user with public key h take a random polynomial $\phi(x) \in R$ and compute $c = p \cdot \phi \cdot h + m$ in R/q.

   To decrypt ciphertext $c \in R/q$ use private key f and compute $a = f \cdot c$ in R/q, choosing coefficients in $[-(q-1)/2, (q-1)/2]$. [If you're a mathematician, lift a to R, i.e. forget about the reduction modulo q]. Then compute $m' = a \cdot f_p$ in R/p, taking coefficients from $[-(p-1)/2, (p-1)/2]$.

   (a) Let $f(x) = x^6 - x^3 + x \in R$.
   Compute $(91x^6 + 35x^5 + 52x^4 + 28x^3 + 42x^2 + 63x + 94) \cdot (x^6 - x^3 + x)$ in R/q to verify that $f_q = 91x^6 + 35x^5 + 52x^4 + 28x^3 + 42x^2 + 63x + 94$. 3 points

   (b) Compute the inverse of $f = x^6 - x^3 + x$ in R/p.
   Hint: this needs a XGCD computation. Make sure to document the steps or state how you did this computation. Do *not* simply state the result or just a verification of the result. 7 points

   (c) Your secret key is $f = x^6 - x^3 + x$; you have computed
   $f_p = -x^6 + x^5 + x^4 - x^3 + 1$ in setting up your key.
   Somebody sends you ciphertext $c = 6x^5 + 4x^4 + 3x^3 + 92x + 99$.
   Compute m'. 6 points

   (d) Show that the system correctly recovers the message, i.e. $m = m'$ if f, g, and ϕ are very sparse and small, i.e. have very few non-zero coefficients chosen from $\{-1, 1\}$ and m has coefficients in $[-(p-1)/2, (p-1)/2]$.
   For the parameters given here, g and ϕ each have one coefficient equal to 1 and one equal to -1. 10 points