TECHNISCHE UNIVERSITEIT EINDHOVEN
Faculty of Mathematics and Computer Science
Exam Cryptology, Wednesday 14 December 2016

Name :

Home university :

Student number :

Exercise	1	2	3	4	5	6	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 6 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 the paper provided; 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 (other than those provided) and cell phones is forbidden.

1. This problem is about RSA encryption.
   (a) Alice chooses $p = 457$ and $q = 383$. Compute Alice's public key (n, e), using $e = 5$, and the matching private key d. 2 points
   (b) Bob uses public key $(n, e) = (101617, 7)$ and secret key $d = 57703$. He receives ciphertext $c = 26497$.
   Decrypt the ciphertext. 1 points
2. This problem is about the Diffie-Hellman key exchange. The system uses the multiplicative group $\mathbb{F}_p^*$ modulo the prime $p = 4327$. The element $g = 3 \in \mathbb{F}_{4327}^*$ has order 4326 and is thus a generator of the full multiplicative group.
   (a) Alice chooses $a = 333$ as her secret key. Compute Alice's public key. 1 point
   (b) Alice receives $h_b = 3107$ from Bob as his Diffie-Hellman keyshare. Compute the key shared between Alice and Bob, using Alice's secret key from the first part of this exercise. 2 points
3. This exercise is about computing discrete logarithms in the multiplicative group of $\mathbb{F}_p$ for some prime p.
   (a) Let $p = 1249$ and note that $p - 1 = 2^5 \cdot 3 \cdot 13$. A generator of $\mathbb{F}_p^*$ is $g = 7$. Bob's public key is $h_b = g^b = 1195$.
   Use the Pohlig-Hellman attack to compute Bob's secret key b; make sure to handle each power of 2 separately as in the algorithm description. Verify your answer, i.e., compute g^b. 12 points
   (b) Let $p = 4327$, so $p - 1 = 2 \cdot 3 \cdot 7 \cdot 103$. Charlie's public key is $h_c = g^c = 172$. You notice that $h_c^{103} = 1$, so, Charlie's secret c is a multiple of 42. Use the Baby-Step Giant-Step attack in the subgroup of order 103 to compute Charlie's secret c. Verify your answer, i.e., compute g^c.
   Hint: Do not forget to include that c is a multiple of 42. 13 points

4. This exercise is about factoring $n = 101617$.

   (a) Use Pollard's rho method for factorization to find a factor of 101617 with iteration function $x_{i+1} = x_i^2 + 11$ and Floyd's cycle finding method, i.e. after each increment in i compute $\gcd(x_{2i} - x_i, 101617)$ until a non-trivial gcd is found. Start with $x_0 = 5$.

   12 points

   (b) Use the $p-1$ method to factor $n = 101617$ with basis $a = 2$ and exponent $s = \text{lcm}\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13\}$. Make sure to determine both factors of n. 5 points

5. (a) Find all affine points, i.e. points of the form (x, y), on the Edwards curve

   $$x^2 + y^2 = 1 + 12x^2y^2$$

   over $\mathbb{F}_{17}$ and state the number of points. 10 points

   (b) Verify that $P = (5, 4)$ is on the curve. Compute the order of P.

   Hint: You may use information learned about the order of points on Edwards curves. 13 points

   (c) Translate the curve **and** P to Montgomery form

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

   i.e. compute A, B and the resulting point P'.

   Verify that the resulting point P' is on the Montgomery curve.

   6 points

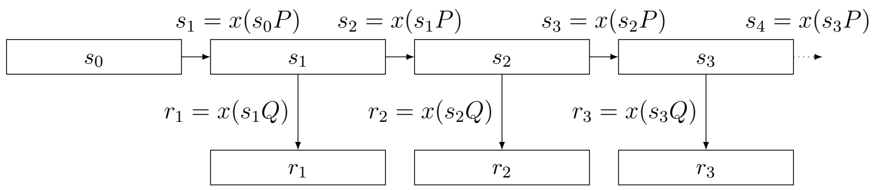
6. In 2006 NIST, the National Institute for Standards and Technology, standardized Dual EC as a method to generate pseudo random numbers. A Pseudo-Random Number Generator (PRNG) is an algorithm that takes as input an integer (or finite field element) and turns it into a long sequence of integers that should be unpredictable based on previous outputs, if the initial input is secret.

   The "EC" in Dual EC stands for Elliptic Curve. The following gives a slightly simplified description of Dual EC but the attack you will find works on deployed versions with small modifications.

Let $E : y^2 = x^3 + ax + b$ be an elliptic curve over $\mathbb{F}_p$, with p prime. Let P be a a point on $E(\mathbb{F}_p)$ of prime order ℓ and let $Q = kP$ for some integer k. Typical sizes are that p and ℓ have 256 bits and k is a random positive integer less than ℓ.

The input s_0 to Dual EC is an integer. The first step is to compute s_0P, take the x-coordinate of s_0P and lift that to an integer s_1. Elements of $\mathbb{F}_p$ are represented as integers in $[0, p-1]$; in the following we no longer explicitly state the process of lifting from an element of $\mathbb{F}_p$ to an integer.

To compute the ith output, $i \geq 1$, two elliptic curve operations happen: First, compute and output $r_i = x(s_iQ)$, i.e., compute s_iQ and then take the x-coordinate, and output the matching integer. Second, compute $s_{i+1} = x(s_iP)$. Here is a schematic drawing of the functions. The values r_i are the output values; the s_i are kept internal. If an attacker learns s_i he can predict all future outputs.



(a) Attacker Eve knows all details about Dual EC, including the curve E, points P and Q and scalar k. She does not know the initial secret s_0. She observes $r_1, r_2, \ldots$ Show how she can compute s_4.
Hint: We did not cover computation of square roots in class, but it is an easy computation. 6 points

(b) Let $p = 401$. The elliptic curve $E : y^2 = x^3 - 3x + 6$ over $\mathbb{F}_p$ has prime order $\ell = 397$. The point $P = (49, 94)$ has order ℓ; let $Q = 265P = (16, 92)$.

You observe $r_1 = 146$. A square-root computation shows you that r_1 comes from the point $s_1Q = \pm(146, 273)$.

Compute s_2. 14 points

(c) Attacker Donald knows p and E but not the points P and Q and scalar k. He observes that the outputs of some PRNG are integers less than p but he is not sure that the PRNG uses Dual EC.

Show how he can distinguish Dual EC output from random elements of $\mathbb{F}_p$. 3 points