TECHNISCHE UNIVERSITEIT EINDHOVEN
Faculty of Mathematics and Computer Science
Exam Cryptology, Tuesday 23 January 2018

Name :

TU/e 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 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.

1. This problem is about the Diffie-Hellman key exchange. The system uses the multiplicative group $\mathbb{F}_p^*$ modulo the prime $p = 23431$. The element $g = 3 \in \mathbb{F}_{23431}^*$ has order 23430 and is thus a generator of the full multiplicative group.

   (a) Alice chooses $a = 365$ as her secret key. Compute Alice's public key. **2 points**

   (b) Alice receives $h_b = g^b = 5252$ from Bob as his Diffie-Hellman keyshare.
   Compute the key shared between Alice and Bob, using Alice's secret key a from the first part of this exercise. **2 points**

2. This problem is about RSA encryption.

   (a) Alice chooses $p = 491$ and $q = 457$. Compute Alice's public key (n, e), using $e = 2^{16} + 1$, and the matching private key d.
   Remember that d is positive. **2 points**

   (b) Bob uses public key $(n, e) = (408257, 11)$ and secret key $d = 184991$. He receives ciphertext $c = 24534$.
   Decrypt the ciphertext. **2 points**

   (c) Decrypt the same message as under b) but this time using RSA with CRT for $p = 647$ and $q = 631$. Make sure to document your computation, i.e., state the values for $c_p, d_p, \ldots$ **5 points**

3. This exercise is about computing discrete logarithms in the multiplicative group of $\mathbb{F}_p$ for $p = 23431$. The element $g = 3$ has order $\ell = 23430$. The factorization of $p-1$ is $p-1 = 2 \cdot 3 \cdot 5 \cdot 11 \cdot 71$. Use the Pohlig-Hellman attack to compute the discrete logarithm b of Bob's key $h_b = g^b = 5252$, i.e.

   (a) Compute b modulo 2. **2 points**

   (b) Compute b modulo 3. **2 points**

   (c) Compute b modulo 5. **4 points**

   (d) Compute b modulo 11. **4 points**

   (e) Compute b modulo 71 using the Baby-Step Giant-Step attack in the subgroup of order 71. Remember to first compute the correct elements of order 71. **8 points**

   (f) Combine the results above to compute b.
   Verify your answer. **4 points**

4. This exercise is about factoring $n = 408257$.

   (a) Use the $p-1$ method to factor $n = 408257$ with basis $a = 5$ and exponent $s = \text{lcm}\{1, 2, 3, 4, 5, 6, 7\}$. Make sure to state the value for s and the result of the exponentiation modulo n. Determine both factors of n. 3 points

   (b) Use Pollard's rho method for factorization to find a factor of 323 with iteration function $x_{i+1} = x_i^2 + 1$ and Floyd's cycle finding method, i.e. after each increment in i compute $\gcd(x_{2i} - x_i, 323)$ until a non-trivial gcd is found. Start with $x_0 = 3$. 6 points

   (c) Use the result of a) and b) to explain why the factorization in a) was successful. This needs statements about why the two primes were separated for this choice of a and s. Note that $631 - 1 = 2 \cdot 3^2 \cdot 5 \cdot 7$ (factored completely) and $647 - 1 = 2 \cdot 323$. 4 points

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

$$x^2 + y^2 = 1 + 6x^2y^2$$

   over $\mathbb{F}_{17}$. 9 points

   (b) Verify that $P = (2, -3)$ is on the curve. Compute the order of P.
   Hint: You may use information learned about the order of points on Edwards curves. 8 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

   (d) The point $Q = (14, 16)$ is on the Montgomery curve with $A = 4, B = 6$ over $\mathbb{F}_{17}$. Compute $3Q$. 8 points

6. RaCoSS is a signature system submitted to NIST's post-quantum competition. The system is specified via two parameters n and $k < n$ and the general system setup publishes an $(n-k) \times n$ matrix H over $\mathbb{F}_2$.

   Alice picks an $n \times n$ matrix over $\mathbb{F}_2$ in which most entries are zero. This matrix S is her secret key. Her public key is $T = H \cdot S$.

   RaCoSS uses a special hash function h which maps to very sparse strings of length n, where very sparse means just 3 non-zero entries for the suggested parameters of $n = 2400$ and $k = 2060$. You may assume that h reaches all possible bitstrings with exactly 3 entries and that they are attained roughly equally often.

   To sign a message m, Alice first picks a vector $y \in \mathbb{F}_2^n$ which has most of its values equal to zero. Then she computes $v = Hy$. She uses the special hash function to hash v and m to a very sparse $c \in \mathbb{F}_2^n$. Finally she computes $z = Sc + y$ and outputs (z, c) as signature on m.

   To verify (z, c) on m under public key T, Bob does the following. He checks that z does not have too many nonzero entries. The threshold here is chosen so that properly computed $z = Sc + y$ pass this test. For numerical values see below. Then Bob computes $v_1 = Hz, v_2 = Tc$ and puts $v' = v_1 + v_2$. He accepts the signature if the hash of v' and m produces the c in the signature.

   (a) Verify that $v' = v$, i.e. that properly formed signatures pass verification. As above, you should assume that the other test on z succeeds.
   Note: All computations take place over $\mathbb{F}_2$. [4 points]

   (b) The concrete parameters in the NIST submission specify that $n = 2400$, and that the output of h has exactly 3 entries equal to 1 and the remaining 2397 entries equal to 0.

   Compute the size of the image of h, i.e., the number of bitstrings of length n that can be reached by h. [4 points]

   (c) Based on your result under b) compute the costs of finding collisions and the costs of finding a second preimage. [4 points]

   (d) For the proposed parameters the threshold for the number of nonzero entries in z is larger than 1000.

   Break the scheme without using any properties of the hash function, i.e. find a way to compute a valid signature (z, c) for any message m and public key T. You have access to the matrix H

and can call h. **Hint:** You can construct a vector z of weight no larger than $n-k$ that passes all the tests. 7 points