TECHNISCHE UNIVERSITEIT EINDHOVEN
Faculty of Mathematics and Computer Science
Exam Cryptology, Tuesday 01 November 2016

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 RSA encryption.

   (a) Alice chooses $p = 439$ and $q = 349$. Compute Alice's public key (n, e), using $e = 5$, and the matching private key d. [2 points]

   (b) Bob uses public key $(n, e) = (153721, 3)$ and secret key $d = 101955$. He receives ciphertext $c = 74088$.
   Decrypt the ciphertext. [2 points]

2. This problem is about the Diffie-Hellman key exchange. The system uses the multiplicative group $\mathbb{F}_p^*$ modulo the prime $p = 1249$. The element $g = 7 \in \mathbb{F}_{1249}^*$ has order 1248 and is thus a generator of the full multiplicative group.

   (a) Alice chooses $a = 234$ as her secret key. Compute Alice's public key. [1 point]

   (b) Alice receives $h_b = 1195$ 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 $p = 709$. The element $g = 551$ has order $\ell = 59$. Charlie uses the subgroup of $\mathbb{F}_{709}^*$ generated by this generator g and you observe him sending $h_c = g^c = 147$. Use the Baby-Step Giant-Step attack in the group generated by g (of size $\ell = 59$) to compute c. [11 points]

4. This exercise is about factoring $n = 171113$.

   (a) Use Pollard's rho method for factorization to find a factor of 171113 with iteration function $x_{i+1} = x_i^2 + 1$ and Floyd's cycle finding method, i.e. after each increment in i compute $\gcd(x_{2i} - x_i, 171113)$ until a non-trivial gcd is found. Start with $x_0 = 7$. [9 points]

   (b) Use the $p - 1$ method to factor $n = 171113$ with basis $a = 16$ and exponent $s = \mathrm{lcm}\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13\}$. 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
$$x^2 + y^2 = 1 + 5x^2y^2$$
over $\mathbb{F}_{13}$. | 9 points |

   (b) Verify that $P = (5, 3)$ is on the curve. Compute the order of P.
Hint: You may use information learned about the order of points on Edwards curves. | 10 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 $Q = (6, 4)$ is on the Montgomery curve with $A = 10, B = -1$ over $\mathbb{F}_{13}$. Compute $3Q$. | 10 points |

6. This exercise is about Diffie-Hellman (DH) key exchange in finite fields. As we have seen in class, index calculus attacks on the DLP in $\mathbb{F}_p^*$ are faster than Pollard's rho attack, so implementations use smaller subgroups or limit the exponent.

   DSA typically specifies three parameters (p, ℓ, g): p is the modulus, meaning that the group $\mathbb{F}_p^*$ is used, and ℓ is the order of the subgroup generated by g. These groups can also be used in DH applications. The implementer is expected to use g as the generator and to choose secret keys smaller than ℓ.

   (a) Alice sends Bob a request to use her preferred parameter set $(234917, 281, 19452)$. However, Bob's library expects only two arguments and reads Alice's parameters as $p = 234917$ and $g = 281$. Bob uses a secret $b < 400$ and sends his DH share $h_b = g^b = 92646$. Compute Bob's b without resorting to a brute force attack.
Verify your solution.
Hint: You might find the factorization of $p - 1 = 2^2 \cdot 11 \cdot 19 \cdot 281$ useful. Note that this g has order $117458 = 2 \cdot 11 \cdot 19 \cdot 281$.
Hint 2: You know everything to run this attack. | 12 points |

(b) Alice sends Bob a request to use her preferred parameter set $(234977, 1049, 202367)$. However, Bob's library expects only two arguments and reads Alice's parameters as $p = 234977$ and $g = 1049$. Bob uses a secret $b < 400$ and sends his DH share $h_b = g^b = 7409$. Compute Bob's b without resorting to a brute force attack.
Verify your solution.
Hint: You might find the factorization of $p-1 = 2^5 \cdot 7 \cdot 1049$ useful. Note that this g has order $117488 = 2^4 \cdot 7 \cdot 1049$. 13 points

(c) Eve knows that Charlie's server uses group 23 from RFC 5114, i.e., a 2048-bit prime p to be used with a subgroup of prime order ℓ, where ℓ has 224-bits. The factorization of $(p-1)/\ell = 2 \cdot 3^2 \cdot 5 \cdot 43 \cdot 73 \cdot 157 \cdot 387493 \cdot 605921 \cdot 742327609 \cdot 5213881177 \cdot 112486462861 \cdot 3528910760717 \cdot C489$, where $C489$ is the product of 3 larger primes. Charlie's server uses static DH, that means the same value of c for all connections. Eve can easily see this by Charlie offering the same $h_c = g^c$ for all connections. This means, that Eve can send Charlie input values $h = g^e$ and Charlie will reply with an AES encryption of `ACKNOWLEDGE` under key $\text{hash}(h^c)$.

Furthermore, Eve knows what software Charlie's server uses and she knows that it does not verify the order of the input values it receives from users.

Describe an attack with which Eve can compute Charlie's secret c in time less than 2^{64}. State the number of queries, i.e. the number of values h_i that Eve sends, and describe how she should choose these values h_i? How much computation does Eve need to do? Note that Charlie's c has 224 bits. 8 points