TECHNISCHE UNIVERSITEIT EINDHOVEN
Faculty of Mathematics and Computer Science
Exam Coding Theory and Cryptology I
Tuesday 15 April 2014

Name :

Student number :

Exercise	1	2	3	4	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 4 exercises. You have from 14:00 – 17:00 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. 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. The binary Hamming code $\mathcal{H}_4(2)$ has parity check matrix

$$H = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$$

and parameters $[15, 11, 3]$.

   (a) Correct the word $(0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1)$. [4 points]

   (b) State the weight enumerator polynomials of $\mathcal{H}_4(2)$ and its dual, the simplex code of length 15. Make sure to expand the expressions. [6 points]

   (c) State the parameters of the second order Reed-Muller code $\mathcal{RM}(2, 4)$ of length $16 = 2^4$. [2 points]

   (d) What do the Gilbert-Varshamov, Singleton, Griesmer, and Hamming bound say about the minimum distance of a binary, linear code of length 15 and dimension 11. [10 points]

   (e) State the parameters (length, dimension, minimum distance) of the punctured $\mathcal{RM}(2, 4)$ code. [2 points]

   (f) State the parameters of the 2^{11}-ary Hamming code with redundancy 2. Give the parameters of the concatenated code that one obtains when using $\mathcal{RM}(2, 4)$ as inner code and the 2^{11}-ary Hamming code with redundancy 2 as outer code. [5 points]

2. This exercise is about factoring $n = 4015$.

   (a) Use Pollard's rho method of factorization to find a factor of 4015. Use starting point $x_0 = 7$, iteration function $x_{i+1} = x_i^2 + 1$ and Floyd's cycle finding method, i.e. compute $\gcd(x_{2i} - x_i, 4015)$ until a non-trivial gcd is found. [8 points]

   (b) Perform one round of the Fermat test with base $a = 2$ to test whether 365 is prime. What is the answer of the Fermat test? [5 points]

   (c) Use Pollard's $p - 1$ factorization method to factor the number $m = 365$ with base $u = 2$ and exponent $s = \text{lcm}\{1, 2, 3, 4\}$. [5 points]

3. (a) Find all affine points on the Edwards curve $x^2 + y^2 = 1 - 7x^2y^2$ over $\mathbb{F}_{17}$. | 10 points |

   (b) Verify that $P = (3, 6)$ is on the curve. Compute $5P$. | 12 points |

   (c) Translate the curve and P to Montgomery form

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

   | 5 points |

4. This exercise is about a signature scheme due to Rabin. The signature scheme relies on the hardness of computing square roots modulo composite numbers. A public key is an RSA modulus $n = p \cdot q$, where both p and q are congruent to 3 modulo 4; p and q constitute the secret key.

   For primes which are congruent to 3 modulo 4 one can compute the square root of a as $a^{(p+1)/4} \bmod p$, if a is a square. You will prove this in the last part of this exercise but should use it in Part 4c.

   Let h be a cryptographic hash function. To sign a message m the signer computes a square root r of $h(m)$ modulo n, if $h(m)$ is a square, and of $-h(m)$ otherwise. To verify the signature, the recipient computes $r^2 \bmod n$ and compares the value to $h(m)$.

   (a) Let $p = 19$. Find all squares in $\mathbb{F}_p$, i.e. find all $a \in \mathbb{F}_p$ so that there exists a $b \in \mathbb{F}_p$ with $a = b^2$. | 3 points |

   (b) Let $p = 19$. For all squares in $\mathbb{F}_p$ (see previous part) compute $a^{(p+1)/4} \bmod p$, compare the results to the values of b obtained above to see which square root is computed. | 3 points |

   (c) Your secret key is $p = 19, q = 23$. Compute the signature on a message for which $h(m) = 220$.
   Hint: You need to do computations modulo p and q separately, and then combine the result using the Chinese Remainder Theorem. | 10 points |

   (d) Show that for a prime p with $p \equiv 3 \bmod 4$ the computation of $a^{(p+1)/4} \bmod p$ computes the square root of a, if a is a square. | 10 points |