**TECHNISCHE UNIVERSITEIT EINDHOVEN**
**Faculty of Mathematics and Computer Science**
# Exam Coding Theory and Cryptology I
**Tuesday 28 January 2014**

Name :

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 14:00 – 17:00 to solve them. You can reach 50 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.

1. The binary Hamming code $\mathcal{H}_3(2)$ has parity check matrix

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

and parameters $[7, 4, 3]$.

(a) Correct the word $(0, 1, 1, 0, 1, 1, 1)$. **2 points**

(b) State the weight enumerator polynomials of $\mathcal{H}_3(2)$ and its dual, the simplex code of length 7. **3 points**

(c) State the parameters of the first order Reed-Muller code $\mathcal{RM}(1, 3)$ of length $8 = 2^3$. **1 point**

(d) What do the Gilbert-Varshamov, Singleton, Griesmer, and Hamming bound say about the minimum distance of a binary, linear code of length 7 and dimension 4. **4 points**

(e) State the parameters (length, dimension, minimum distance) of the punctured $\mathcal{RM}(1, 3)$ code. **1 point**

(f) State the parameters (length, dimension, minimum distance) of the code obtained by the $(u, u + v)$ construction with $u \in \mathcal{H}_3(2)$ and $v$ in the punctured $\mathcal{RM}(1, 3)$ code. **1 point**

(g) Give the parameters of the concatenated code that one obtains when using $\mathcal{RM}(1, 3)$ as inner code and a $2^4$-ary Hamming code with redundancy 3 as outer code. **3 points**

2. This exercise is about factoring $n = 2014$. Obviously, 2 is a factor, so the rest of the exercise is about factoring the remaining factor $m = 2014/2 = 1007$.

   (a) Use Pollard's rho method of factorization to find a factor of 1007. Use starting point $x_0 = 1$, iteration function $x_{i+1} = x_i^2 + 1$ and Floyd's cycle finding method, i.e. compute $\gcd(x_{2i} - x_i, 1007)$ till a non-trivial gcd is found.

   5 points

   (b) Perform one round of the Fermat test with base $a = 2$ to test whether 19 is prime. What is the answer of the Fermat test?

   2 points

   (c) Use Pollard's $p-1$ factorization method to factor the number $n = 1007$ with base $u = 2$ and exponent $2^3 \cdot 3^2$.

   3 points

3. (a) Find all affine points on the Edwards curve $x^2 + y^2 = 1 - 5x^2y^2$ over $\mathbb{F}_{13}$.

   4 points

   (b) Verify that $P = (6, 3)$ is on the curve. Compute the order of $P$.

   4 points

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

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

   2 points

4. The curve $y^2 = x^3$ is not an elliptic curve over $\mathbb{F}_{71}$ but the set of points $\{(x, y) | x, y \in \mathbb{F}_{71}^*, y^2 = x^3\} \cup \{P_\infty\}$ forms a group under the addition and doubling laws on (short) Weierstrass curves.

   (a) The point $(1, 1)$ is on the curve. Compute $2P, 3P, 4P$, and $8P$.

   6 points

   (b) Compute the fractions $x/y$ for $2P, 3P, 4P$, and $8P$.

   2 points

   (c) Compute the discrete logarithm of $(6, 43)$ with base $(1, 1)$. Make sure to justify your approach.

   7 points