TECHNISCHE UNIVERSITEIT EINDHOVEN
Faculty of Mathematics and Computer Science
Exam Coding Theory and Cryptology I
Friday 27 January 2012

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 simple, non-graphical pocket calculator. Usage of laptops and cell phones is forbidden.

1. What do the Gilbert-Varshamov, Singleton, Griesmer, and Hamming bound say about the dimension of a binary, linear code of length 11 and minimum distance 5. $\boxed{\text{5 points}}$

2. Let the public key of user U in the McEliece system be

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

over $\mathbb{F}_2$ and let $w = 1$ (the number of errors one can add in the encryption). Demonstrate the usage of the McEliece cryptosystem by encrypting $m = (1\,0\,0)$. $\boxed{\text{4 points}}$

3. This exercise is about constructing codes starting from a Hamming code. Let C be a binary Hamming code of dimension 4.

   (a) State the parameters (length, dimension, redundancy, minimum distance) and parity check matrix of C. $\boxed{\text{2 points}}$

   (b) State the parameters (length, dimension, minimum distance) and parity check matrix of the extended code C^{ext} of C. $\boxed{\text{2 points}}$

   (c) Give the parameters of the concatenated code that one contains when using C^{ext} as inner code and a 2^4-ary Hamming code with redundancy 3 as outer code. $\boxed{\text{5 points}}$

4. This exercise is about computing discrete logarithms in some groups.

   (a) The integer $p = 10037$ is prime. You are the eavesdropper and know that Alice and Bob use the Diffie-Hellman key-exchange in a cyclic subgroup of $(\mathbb{Z}/p, +)$ with generator $g = 1234$. You observe $h_a = 2345$ and $h_b = 4567$. What is the shared key of Alice and Bob? $\boxed{\text{4 points}}$

   (b) The order of 5 in $\mathbb{F}_{73}^*$ is 72. Charlie uses the subgroup generated by $g = 5$ for cryptography. His public key is $g_c = 2$. Use the Pohlig-Hellman method to compute an integer c so that $g_c \equiv g^c \bmod 73$. $\boxed{\text{10 points}}$

5. (a) Find all affine points on the Edwards curve $x^2 + y^2 = 1 - 3x^2y^2$ over $\mathbb{F}_{11}$. **4 points**

   (b) Verify that $P = (2, 2)$ is on the curve. Compute the order of P. **3 points**

   (c) Translate the curve and P to Montgomery form
   $$Bv^2 = u^3 + Au^2 + u.$$
   2 points

6. The Hill cipher is a secret-key system based on matrices. It takes a message in the English alphabet (26 characters), translates the characters into numbers as given below, and then encrypts the message by encrypting n numbers at a time as follows:
   Let the secret key M be an $n \times n$ matrix over $\mathbb{Z}/26\mathbb{Z}$ which is invertible and let the plaintext a be the vector $(a_1, a_2, \ldots, a_n) \in (\mathbb{Z}/26\mathbb{Z})^n$. The corresponding ciphertext is $c^T = Ma^T$. To decrypt compute $a^T = M^{-1}c^T$.

   (a) Let
   $$M = \begin{pmatrix} 2 & 1 & 1 \\ 1 & 3 & 2 \\ 1 & 3 & 1 \end{pmatrix}.$$
   Encrypt the text `CRY PTO`
   3 points

   (b) Let M be a 2×2 matrix. You know that $(1, 3)^T$ was encrypted as $(-9, -2)^T$ and that $(7, 2)^T$ was encrypted as $(-2, 9)^T$. Find the secret key M.
   6 points

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25