TECHNISCHE UNIVERSITEIT EINDHOVEN
Faculty of Mathematics and Computer Science
Exam Coding Theory and Cryptology I
Friday 13 April 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. Use the Griesmer bound to determine the maximal dimension of a binary, linear code of length 101 and minimum distance 50. 2 points

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

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

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 $m = (0\,1\,1)$. 3 points

3. This exercise is about constructing codes starting from some given ones. Let C_1 be the Reed-Muller code RM(r, m)=RM$(2, 3)$ and let C_2 be the binary Hamming code with $[n, k, d] = [7, 4, 3]$.

   (a) State the parameters (length, dimension, and minimum distance) of C_1. 1 point

   (b) Let C_1' be the code obtained from C_1 by puncturing. State the parameters (length, dimension, and minimum distance) of this code C_1'. Note: determine the exact value of d. 1 point

   (c) State the parameters (length, dimension, minimum distance) of the code obtained by the $(u, u + v)$ construction with $u \in C_1'$ and $v \in C_2$. Call the resulting code C_3. 2 points

   (d) The code C_3 constructed in the previous part of the exercise will now be used as inner code in a concatenated code. Let C_4 be a Hamming code with redundancy $r = 3$ over an appropriately sized field so that it can be used as an outer code for C_3. State the parameters for C_4 and for the concatenated code. Note: if you did not solve the previous part of the exercise assume that C_3 has parameters $[n_3, k_3, d_3]$. 5 points

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

   (a) The integer $p = 17$ is prime. You are the eavesdropper and know that Alice and Bob use the Diffie-Hellman key-exchange in $\mathbb{F}_{17}^*$ with generator $g = 3$. You observe $h_a = 12$ and $h_b = 14$. What is the shared key of Alice and Bob? 5 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 Baby-Step Giant-Step method to compute an integer c so that $g_c \equiv g^c \bmod 73$.

10 points

5. (a) Find all affine points on the twisted Edwards curve $-x^2 + y^2 = 1 - 3x^2y^2$ over $\mathbb{F}_{17}$. 5 points

(b) Verify that $P = (6, 10)$ is on the curve. Compute $4P$. 4 points

(c) Translate the curve and P to Montgomery form

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

2 points

6. In 1995 Shamir suggested an improvement to RSA called "RSA for paranoids". In this system encryption and decryption work the usual way with $c \equiv m^e \bmod n$ and $m \equiv c^d \bmod n$ but the primes p and q have significantly different sizes – for an 80-bit security level p has the usual 500 bits while q has 4500 bits. This means that the attacker is faced with the problem of factoring a huge number. There is also some performance hit for the sender of a message since he has to work modulo a larger number $n = pq$, but Shamir is nice enough to limit the size of the messages m to be smaller than p and to suggest a small-ish encryption exponent such as $e = 23$.

(a) Explain why in the above scenario $e = 3$ would lead to an insecure system.

2 points

(b) Explain how the use of these parameters $m < p \ll q$ speeds up decryption.

Hint: You do not need to determine q. 4.5 points

(c) Decipher the ciphertext $c = 187008753$ knowing that $e = 17, p = 11, n = 214359541$.
Hint: You are likely to do some modular reduction by hand for this one, I do not expect your pocket calculator to handle computations modulo n. 3.5 points