TECHNISCHE UNIVERSITEIT EINDHOVEN
Faculty of Mathematics and Computer Science
Exam Coding Theory and Cryptology I
Tuesday 27 January 2015

Name : 
Student number : 

<table>
<thead>
<tr>
<th>Exercise</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>total</th>
</tr>
</thead>
<tbody>
<tr>
<td>points</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Notes: Please hand in this sheet at the end of the exam. You may keep the sheets with the exercises. This exam consists of 5 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 exercise is about binary codes.

(a) State the parameters of the second order Reed-Muller code $\mathcal{R}\mathcal{M}(2, 4)$ of length $16 = 2^4$.

(b) Let $c$ be a codeword of Hamming weight $d = 4$ in $\mathcal{R}\mathcal{M}(2, 4)$. State the parameters of $C_{\text{res}}$, the residual code of $\mathcal{R}\mathcal{M}(2, 4)$ with respect to $c$.

(c) Use the Griesmer bound to compute the minimum distance of $C_{\text{res}}$, the residual code from exercise 1.b).

2. This exercise is about ternary ($q = 3$) BCH codes of length $n = 13$. Let $\alpha$ be a primitive $n$-th root of unity.

(a) Let $C$ be a narrow-sense BCH code with designed distance $d = 3$. State the defining set of $C$ and compute a lower bound on the minimum distance of $C$.

(b) For all $0 \leq i < 13$ compute the cyclotomic cosets $C_i$ (with respect to $\alpha$).

(c) Let $C'$ be a BCH code (not necessarily narrow-sense) with designed distance $d = 3$ and a defining set that is minimal for this distance. State such a minimal defining set of $C'$ and compute a lower bound on the minimum distance of $C'$.

(d) What do the Gilbert-Varshamov, Singleton, and Hamming bound say about the dimension of a ternary, linear code of length $n = 13$ and minimum distance $d = 3$?

3. This exercise is about factoring $n = 2015$. Obviously, 5 is a factor, so the rest of the exercise is about factoring the remaining factor $m = 2015/5 = 403$.

(a) Use Pollard’s rho method of factorization to find a factor of 403. Use starting point $x_0 = 2$, iteration function $x_{i+1} = x_i^2 + 1$ and Floyd’s cycle finding method, i.e. compute $\gcd(x_{2i} - x_i, 403)$ until a non-trivial $\gcd$ is found. Make sure to document the intermediate steps.
(b) Perform one round of the Fermat test with base $a = 2$ to test whether 31 is prime. What is the answer of the Fermat test?  
2 points

(c) Perform one round of the Miller-Rabin test with base $a = 2$ to test whether 31 is prime. What is the answer of the Miller-Rabin test?  
4 points

(d) Use Dixon’s factorization method to factor the number $n = 403$ using $a_1 = 22$.  
6 points

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

(b) Verify that $P = (3, 4)$ is on the curve. Compute the order of $P$.  
8 points

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

5. This exercise introduces the Paillier cryptosystem. Key generation works similar to that in RSA: Let $p$ and $q$ be large primes, put $n = pq$, $g = n + 1$, and compute $\varphi(n) = (p-1)(q-1)$ and $\mu \equiv \varphi(n)^{-1} \mod n$. The public key is $(n, g)$, the private key is $(\varphi(n), \mu)$.

To encrypt message $m \in \mathbb{Z}/n$ pick a random $1 \leq r < n$ with $\gcd(r, n) = 1$ and compute the ciphertext $c \equiv g^m \cdot r^n \mod n^2$. Note the computation is done modulo $n^2$, not modulo $n$.

To decrypt $c \in \mathbb{Z}/n^2$ compute $d \equiv c^{\varphi(n)} \mod n^2$. Consider $d$ as an integer and observe that $d - 1$ is a multiple of $n$ (see below). Compute $e = (d - 1)/n$ and obtain the message as $m \equiv e\mu \mod n$.

(a) Encrypt the message 123 to a user with public key $(n, g) = (4087, 4088)$ using $r = 11$.  
2 points

(b) Your public key is $(n, g) = (3127, 3128)$ and your secret key is $(\varphi(n), \mu) = (3016, 2141)$. Decrypt the ciphertext $c = 8053838$.  
4 points

(c) Compute symbolically (no particular value of $n$ or $r$) $\varphi(n^2)$ and $r^{n\varphi(n)} \mod n^2$, using $n = pq$.  
4 points
(d) Compute symbolically (no particular value of $n$ or $m$)
$$g^{mr(n)} \mod n^2.$$  
4 points

(e) Explain why $d - 1$ is a multiple of $n$ and why decryption recovers $m$.

**Hint:** use the previous two parts.  
4 points

(f) Let $c_1$ be the encryption of $m_1$ using some $r_1$ and let $c_2$ be the encryption of $m_2$ using some $r_2$, both for the same public key $(n, g)$. Show that $c \equiv c_1 c_2 \mod n^2$ decrypts to $m_1 + m_2$.

Make sure to justify your answer.  
10 points