Notes: Please hand in this sheet at the end of the exam. You may keep the sheet 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 problem is about ElGamal encryption in the group $\mathbb{F}_{2003}^*$ with generator $g = 5$.

(a) Alice’s public key is $h = 877$. Encrypt the message $m = 1002$ to Alice using ElGamal encryption with random value $k = 2^{10} + 1$. 4 points

(b) Charlie has private key $c = 123$. He receives ciphertext $(c_1, c_2) = (1410, 1815)$. Decrypt the message. 4 points

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

(a) Alice and Bob use the additive group modulo $p = 1003$ with generator $g = 5$ for their Diffie-Hellman system. You observe the DH shares $a' = a \cdot g = 123$ and $b' = b \cdot g = 456$. Compute their shared secret. 4 points

(b) Use the baby-step-giant-step algorithm to determine Alice’s secret key $a$ for the parameters in exercise 1, i.e. $\mathbb{F}_{2003}^*$, $g = 5$, and $h = 877$.
Make sure to document all intermediate steps. 20 points

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. 8 points

(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 \( r^m \varphi(n) \mod n^2 \), using \( n = pq \).  
4 points
(d) Compute symbolically (no particular value of \( n \) or \( m \)) \( g^{m\varphi(n)} \mod n^2 \).  
4 points
(e) Explain why \( d - 1 \) is a multiple of \( n \) and why decryption recovers \( m \).  
4 points

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

(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 \( c \equiv c_1c_2 \mod n^2 \) decrypts to \( m_1 + m_2 \). Make sure to justify your answer.  
10 points