# TECHNISCHE UNIVERSITEIT EINDHOVEN
## Faculty of Mathematics and Computer Science
## Exam Cryptology, Tuesday 29 October 2024

Name :

TU/e 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 sheets with the exercises.
This exam consists of 6 exercises. You have from 09:00 – 12:00 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, printouts, and notes on paper, 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 personal laptops and cell phones is forbidden. You can use the laptops provided in the exam room.

1. This problem is about RSA encryption. Bob generated his key using primes $p = 613$ and $q = 431$ to get public key $(n, e) = (264203, 65537)$ and private key $(n, d) = (264203, 85553)$.

   (a) Bob receives ciphertext $c = 60437$.
   Decrypt the ciphertext. Verify your answer by re-encrypting the message. [2 points]

   (b) Decrypt the same message as under a) but this time using RSA with CRT. Make sure to document your computation, i.e., state the values for $c_p, d_p, m_p.c_q \ldots$. [5 points]

2. This exercise is about computing discrete logarithms in the multiplicative group of $\mathbb{F}_p$ for $p = 3727$. The element $g = 3$ has order $p-1 = 3726$. The factorization of $p-1$ is $p-1 = 2 \cdot 3^4 \cdot 23$. Use the Pohlig-Hellman attack to compute the discrete logarithm $b$ of Bob's key $h_B = g^b = 3333$, i.e. perform the following steps.

   (a) Compute $b$ modulo 2. [2.5 points]

   (b) Compute $b$ modulo $3^4$, by first computing it modulo 3 and then, using the same table of powers of $g$, computing it modulo $3^2$, then, using the same table of powers of $g$, computing it modulo $3^3$, and finally, using the same table of powers of $g$, computing it modulo $s^4$.
   Verify your answer by verifying the discrete logarithm in the subgroup of order $3^4$. [9.5 points]

(c) Compute $b$ modulo 23 using the Pollard-rho method in the schoolbook version with Floyd's cycle-finding method, on $G = g^{(p-1)/23}$ and $H = h^{(p-1)/23}$. The fast and slow walk both start at $s_0 = f_0 = G \cdot H^2, a_0 = 1, b_0 = 2$.

$$s_{i+1} = \begin{cases} s_i \cdot G \\ s_i \cdot H \\ s_i^2 \end{cases}, a_{i+1} = \begin{cases} a_i + 1 \\ a_i \\ 2a_i \end{cases}, b_{i+1} = \begin{cases} b_i \\ b_i + 1 \\ 2b_i \end{cases} \text{ for } s_i \equiv \begin{cases} 0 \bmod 3 \\ 1 \bmod 3 \\ 2 \bmod 3 \end{cases},$$

where to select the step one takes $s_i$ as an integer in $[0, p-1]$.
The twice as fast walk has $f_i = s_{2i}$.
Document all $s_i$ you compute and verify the answer for $b$ mod 23.
Hint: Remember that you need to wait for a collision between $s_i$ and $f_i$ at the same $i$ even if you see the same values appear already earlier – but the latter still simplifies your computation as you know what step to take next and you see the collision coming.
Here you will need 3 steps. **8 points**

(d) Combine the results above to compute $b$.
Verify your answer.
If you have only two parts of the result combine those and verify your result on the matching subgroup. **4 points**

3. This exercise is about factoring.

(a) Use the $p-1$ method to factor $n = 272123$ with basis $a = 7$ and exponent $s = \text{lcm}\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$. Make sure to state the value for $s$ and the result of the exponentiation modulo $n$. Determine both factors of $n$. **4 points**

(b) The factorization of 540 is $540 = 2^2 \cdot 3^3 \cdot 5$ and that of 502 is $502 = 2 \cdot 251$. Explain why the factorization in (a) was successful and explain what fraction of bases $a$ works to factor $n$ for this $s$. **5 points**

4. (a) Find all affine points, i.e. points of the form $(x, y)$, on the Edwards curve
$$E : x^2 + y^2 = 1 + 7x^2y^2$$
over $\mathbb{F}_{23}$. 11 points

   (b) The point $P = (4, 18)$ is on the curve. Compute the order of $P$.
**Hint:** You may use information learned about the order of points on Edwards curves. Under (a) you should have found 28 points. 9 points

   (c) Translate the curve to Montgomery form **and** compute the image $P'$ of $P$ on that curve
$$M_{A,B} : Bv^2 = u^3 + Au^2 + u,$$
i.e. compute $A$, $B$ and the resulting point $P'$ on $M_{A,B}$.
Verify that the resulting point $P'$ is on the Montgomery curve. 5 points

   (d) In (b) you computed $2P$ on $E$ and in $(c)$ you computed the image $P'$ of $P$ on $M_{A,B}$. Compute the image of $2P$ on $M_{A,B}$ and then on $M_{A,B}$ from (c) double $P'$ to compute $2P'$ directly. Compare the results. 6 points

5. This exercise is about Coppersmith's method to factor $n$ given known parts of the prime $p$.

   (a) Describe in your own words the steps of Coppersmith's method to factor $n = pq$ if the top bits of $p$ are known and the unknown part is in the lowest $b$ bits of $p$. 8 points

   (b) For concreteness, show how to set up the matrix for LLL when using $x^3f(x)^3, x^2f(x)^3, xf(x)^3, f(x)^3, nf(x)^2, n^2f(x)$, and $n^3$. 2 points

   (c) Use your matrix from part (b) and the theorem of Howgrave-Graham to show that $b$ may be up to 3/7 of the bits of $p$ to have LLL guaranteed to recover the missing part of $p$.
You can assume that $p, q \approx \sqrt{n}$.
You can ignore constants that do not scale with $p$. 3 points

6. This exercise is about ElGamal encryption.

   The system works in a group $G$, written multiplicatively in the following way. Typically $G$ is a subgroup of $\mathbb{F}_p^*$ for some prime $p$ given as the powers of some generator $g \in \mathbb{F}_p^*$, i.e., $G = \{g^i | i = 0, 1, \ldots, \ell - 1\}$ for $\ell$ the order of $g$. Messages are assumed to be elements of $G$.

   Here is the definition of ElGamal encryption:

   **KeyGen:** Pick random $0 < a < \ell$, compute $h_A = g^a$.
   The public key is $h_A$, the private key is $a$.

   **Encrypt:** Pick random $0 < k < \ell$, compute $r = g^k$ and $c = m \cdot h_A^k$.
   Send $(r, c)$ as ciphertext.

   **Decrypt:** Compute $m' = c/r^a$

   (a) Show that the system works correctly, i.e., show that $m' = m$.
   2 points

   (b) Show that the system also works correctly if the restriction of $m \in G$ is dropped and instead only $m \in \mathbb{F}_p^*$ is required. 2 points

   (c) Alice uses this system for $p = 30139$ and wants to avoid the Pohlig–Hellman attack and thus chooses generator $g = 17$ which has prime order 5023 in $\mathbb{F}_p^*$. The complete factorization of $p - 1$ is $2 \cdot 3 \cdot \ell$.

   You observe a ciphertext $(r, c) = (740, 959)$ from Bob and know from other information that Bob's message is an integer in $[91, 96]$.

   Determine the message that Bob sent.

   **Hint:** It is a coincidence that $r$ and $c$ are both small compared to $p$; this does not contribute to the solution.

   **Hint 2:** Bob does not seem to restrict his messages to $G$. Note that you can test if the message is in $G$.

   **Hint 3:** The test in Hint 2 should give you some idea of what to look for.

   **Hint 4:** You are not expected to do a DLP computation and you do not need $r$. You will need to do a test for each candidate message.
   12 points