TECHNISCHE UNIVERSITEIT EINDHOVEN
Faculty of Mathematics and Computer Science
Exam Cryptology, Tuesday 31 October 2017

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 sheet with the exercises.
This exam consists of 6 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 the Diffie-Hellman key exchange. The system uses the multiplicative group $\mathbb{F}_p^*$ modulo the prime $p = 23689$. The element $g = 11 \in \mathbb{F}_{23689}^*$ has order 23688 and is thus a generator of the full multiplicative group.

   (a) Alice chooses $a = 222$ as her secret key. Compute Alice's public key. **1 point**

   (b) Alice receives $h_b = g^b = 22938$ from Bob as his Diffie-Hellman keyshare.
   Compute the key shared between Alice and Bob, using Alice's secret key g^a from the first part of this exercise. **2 points**

2. This problem is about RSA encryption.

   (a) Alice chooses $p = 439$ and $q = 349$. Compute Alice's public key (n, e), using $e = 2^{16} + 1$, and the matching private key d. **2 points**

   (b) Bob uses public key $(n, e) = (443507, 11)$ and secret key $d = 241187$. He receives ciphertext $c = 64649$.
   Decrypt the ciphertext. **2 points**

   (c) Decrypt the same message as under b) but this time using RSA with CRT for $p = 659$ and $q = 673$. Make sure to document your computation, i.e., state the values for $c_p, d_p, \ldots$ **4 points**

3. This exercise is about computing discrete logarithms in the multiplicative group of $\mathbb{F}_p$ for $p = 23689$. The element $g = 11$ has order $\ell = 23688$. The factorization of $p - 1$ is $p - 1 = 2^3 \cdot 3^2 \cdot 7 \cdot 47$. Use the Pohlig-Hellman attack to compute the discrete logarithm b of Bob's key $h_b = g^b = 22938$, i.e.

   (a) Compute b modulo 2^3 by first computing b modulo 2, then modulo 2^2 and finally modulo 2^3. **4 points**

   (b) Compute b modulo 3^2 by first computing b modulo 3 and then modulo 3^2. **5 points**

   (c) Compute b modulo 7. **4 points**

   (d) Compute b modulo 47 using the Baby-Step Giant-Step attack in the subgroup of order 47 **7 points**

   (e) Combine the results above to compute b.
   Verify your answer. **4 points**

4. This exercise is about factoring $n = 443507$.

   (a) Use the $p-1$ method to factor $n = 443507$ with basis $a = 13$ and exponent $s = \text{lcm}\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13\}$. Make sure to state the value for s and the result of the exponentiation modulo n. Determine both factors of n. **4 points**

   (b) Use Pollard's rho method for factorization to find a factor of 329 with iteration function $x_{i+1} = x_i^2 + 3$ and Floyd's cycle finding method, i.e. after each increment in i compute $\gcd(x_{2i} - x_i, 329)$ until a non-trivial gcd is found. Start with $x_0 = 3$. **5 points**

   (c) Use the result of b) to explain why the factorization in a) was successful. Note that $673 - 1 = 2^5 \cdot 3 \cdot 7$ (factored completely) and $659 - 1 = 2 \cdot 329$. **3 points**

5. (a) Find all affine points, i.e. points of the form (x, y), on the Edwards curve

$$x^2 + y^2 = 1 + 5x^2y^2$$

   over $\mathbb{F}_{17}$. **9 points**

   (b) Verify that $P = (5, 10)$ is on the curve. Compute the order of P.
   Hint: You may use information learned about the order of points on Edwards curves. **10 points**

   (c) Translate the curve **and** P to Montgomery form

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

   i.e. compute A, B and the resulting point P'.
   Verify that the resulting point P' is on the Montgomery curve. **6 points**

   (d) The point $Q = (1, 16)$ is on the Montgomery curve with $A = 14, B = -1$ over $\mathbb{F}_{17}$. Compute $3Q$. **10 points**

6. Lots of applications in cryptography require random numbers. The *power generator* generates random numbers in $\mathbb{F}_p^*$ by taking random powers of a generator, i.e., computing random number x as $x = g^r$ in $\mathbb{F}_p$ for some fixed g.

(a) Company C wants to generate numbers coprime to $3, 5, 7, 11$, and 13. They choose to pick 5 small random numbers $r_1, r_2, \ldots, r_5$, compute

$$\begin{aligned} x &\equiv 2^{r_1} \bmod 3 \\ x &\equiv 3^{r_2} \bmod 5 \\ x &\equiv 3^{r_3} \bmod 7 \\ x &\equiv 2^{r_4} \bmod 11 \\ x &\equiv 2^{r_5} \bmod 13 \end{aligned}$$

and then combine these five congruences using the Chinese Remainder Theorem (CRT) to a single number x modulo $3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 = 15015$.

Explain why the resulting numbers are coprime to $3, 5, 7, 11$, and 13.

Compute how many different numbers can be generated using this method. **6 points**

(b) Company S wants to simplify the code and picks a single number as generator, so x is computed picking 5 small random numbers $r_1, r_2, \ldots, r_5$ as before and solving the following CRT for x.

$$\begin{aligned} x &\equiv 2^{r_1} \bmod 3 \\ x &\equiv 2^{r_2} \bmod 5 \\ x &\equiv 2^{r_3} \bmod 7 \\ x &\equiv 2^{r_4} \bmod 11 \\ x &\equiv 2^{r_5} \bmod 13 \end{aligned}$$

Compute how many different numbers can be generated using the method of company S. **3 points**

(c) Impatient company I additionally wants to avoid the CRT step and generates numbers coprime to 15015 by taking a larger random number $r < 15015$ and computing

$$x \equiv 5477^r \bmod 15015.$$

Compute how many different numbers can be generated using the method of company I.

Verify your answer. **9 points**