Security

Assignment 8, Friday, November 17, 2017

Handing in your answers:

- Include your name and student number **in** the document (they will be printed!), as well as the name of your teaching assistant (Bart or Joost). When working together, include **both** your names and student numbers.
- Submit one single **pdf** file – when working together, only hand in **once**.
- Hand in via Blackboard, before the deadline.

Deadline: Monday, November 27, 09:00 sharp!

Goals: After completing these exercises successfully you should be able to

- perform basic computations with modular arithmetic;
- reason about generic secrecy properties of public key systems.

Marks: You can score a total of 100 points.

1. **(10 points)**
   (a) Start counting on a Friday. What day will it be in 1000 days? Explain your answer.
   (b) Without using a calculator: what is the last digit of 2^{1893}? Explain how you found it.
2. **(20 points)**
   (a) Write down the multiplication table for $\mathbb{Z}_{10}$ (so, for the set of whole numbers modulo 10), as was done in the course slides for $\mathbb{Z}_5$.
   (b) Which elements of $\mathbb{Z}_{10}$ have an inverse for multiplication in $\mathbb{Z}_{10}$?
   (c) What numbers do not have an inverse modulo 15? Explain how you found these.
3. **(15 points)** Reduce the following expressions to the smallest non-negative representation.
   (a) $169 \mod 11$
   (b) $-10 \mod 6$
   (c) $175 \mod 9$
   (d) $903 - 621 \mod 9$
   (e) $175 \cdot (903 - 621) \mod 9$
4. **(35 points)** In this exercise, we consider prime divisors and the greatest common divisor (notation: $\gcd(x, y)$). As the name suggests, the greatest common divisor of x and y is the largest integer that divides both x and y without remainder (*e.g.* $\gcd(5, 15) = 5$).
   (a) Find the factorization of 210.
   (b) The prime factorization of 75 is $3^1 \cdot 5^2$. Find $\gcd(75, 210)$.
   (c) Find the factorization of this greatest common divisor.
   (d) Factorize 198 and 135.
   (e) Give $\gcd(198, 135)$ in terms of *all* common prime divisors (2, 3, 5, and 11), i.e. use zero exponents in the product when a term is not present.
   (f) Now we generalize our findings in this last exercise. Let $x = p_1^{n_1} \cdot \ldots \cdot p_k^{n_k}$ and $y = p_1^{m_1} \cdot \ldots \cdot p_k^{m_k}$ be the factorizations of x and y, respectively, where prime factors p_i appear at least in one of the prime factorizations of x and y (thus, some of the exponents n_i or m_j may be 0). What is the factorization of $\gcd(x, y)$?

5. **(10 points)** In exercise 3 we already worked with multiplicative inverses. Let's define the concept more precisely. The multiplicative inverse of any integer a modulo n is x such that $x \cdot a \equiv 1 \pmod{n}$. Note that such an x does not always exist.

   (a) Find x such that $x \cdot 13 \equiv 1 \pmod{16}$ holds.

   (b) Without writing down the complete row from the multiplication table: does 12 have an inverse in $\mathbb{Z}_{170}$? Why (not)?

6. **(10 points)** A few weeks ago the one-time pad encryption scheme was discussed. Given a ciphertext produced by that scheme, it is impossible to find the corresponding plaintext without knowing the right key, as *every* plaintext is equally likely (*i.e.* one can easily come up with a key to derive any desired plaintext). The ciphertext leaks no information about the original plaintext whatsoever. This property is called perfect secrecy.

   Can we achieve the same property with a public-key cryptosystem? Explain your answer.