Security

Assignment 8, Wednesday, November 11, 2015

Handing in your answers: the full story, see

`http://www.sos.cs.ru.nl/applications/courses/security2015/exercises.html`

Briefly,

- submission via Blackboard (`http://blackboard.ru.nl`);
- one single pdf file;
- make sure to write all names and student numbers and the name of your teaching assistant (Brinda or Joost).

Deadline: Thursday, November 19, 24:00 (midnight) sharp!

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

- to perform basic computations with modular arithmetic.

Marks: You can score a total of 100 points.

1. **(20 points)**
   (a) Write down the multiplication table for $\mathbb{Z}_9$ (so, for the whole numbers modulo 9), as was done in the course slides for $\mathbb{Z}_5$.
   (b) Which numbers have an inverse for multiplication in $\mathbb{Z}_9$?
   (c) What are the numbers that don't have an inverse modulo 15? Explain how you found these.

2. **(20 points)**
   (a) Reduce the following expressions to the smallest non-negative representation.
      i. 173 mod 7
      ii. -9 mod 6
      iii. 68 mod 17
      iv. $(894 - 573)$ mod 7
      v. $173 \cdot (894 - 573)$ mod 7
   (b) Find z if

$$\begin{aligned} x &\equiv 43 \pmod{47} \\ y &\equiv 46 \pmod{47} \\ x + y &\equiv z \pmod{47}. \end{aligned}$$

3. **(40 points)** In this problem let us 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) The prime factorization of 98 is $2^1 \cdot 7^2$. Find the factorization of 420, then find their greatest common divisor $\gcd(98, 420)$ and its factorization.
   (b) Factorize 66 and 135. Find $\gcd(66, 135)$ and then factorize $\gcd(66, 135)$ in terms of *all* common prime divisors (2, 3, 5, and 11). You can use zero exponents in the product.
   (c) 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 $\gcd(x, y)$?

4. **(10 points)** In Problem 1 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 $13 \cdot x \equiv 1 \pmod{16}$ holds.

(b) Let $a = n - 1$. Find x such that $ax \equiv 1 \pmod{n}$. Show how you found this.

5. **(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.