Security

Assignment 8, Friday, November 11, 2016

Handing in your answers: For the full story, see

`http://www.sos.cs.ru.nl/applications/courses/security2016/exercises.html`

To summarize:

- Include your name and student number **in** the document (they will be printed!), as well as the name of your teaching assistant (Hans 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 21, 09:00 sharp!

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

- perform basic computations with modular arithmetic.

Marks: You can score a total of 100 points.

1. **(10 points)** During the lecture, a protocol was described in which Alice and Bob establish a symmetric key by sharing values via a group of common friends (see slide 8). Alice generates a new 128 bit string (k_i) for each friend, which they then pass on to Bob. Both Alice and Bob construct their shared key by XOR'ing all these parts together: $K = k_0 \oplus k_1 \oplus k_2 \ldots \oplus k_n$.

   To use this protocol with 8 common friends, Alice would need to generate $128 \cdot 8 = 1024$ bits of random data. As she thinks this is too much work, she decides on a different approach: Alice generates a key K of 128 random bits, splits it into chunks k_i of 16 bits each, and simply sends one chunk to each of the common friends. When all friends forward their bits to Bob, he can reconstruct the key by concatenating the chunks: $K = k_0 \| k_1 \| k_2 \ldots \| k_7$.

   (a) Suppose that 7 of the common 'friends' conspire to find the key K. How many possible keys are there? And how many keys would 6 conspiring friends need to try, at most?

2. **(10 points)**

   (a) When you start counting on a Friday, what day of the week will it be in 1000 days? Explain your answer.

   (b) <u>Without using a calculator</u>: what is the last digit of 2^{1893}? Explain how you found it.

3. **(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.

. . . . **The assignment continues on the next page!** . . . .

4. **(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) $175 \cdot (903 - 621) \mod 9$

5. **(30 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) The prime factorization of 75 is $3^1 \cdot 5^2$. Find the factorization of 210, then find their greatest common divisor $\gcd(75, 210)$ 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 $\gcd(x, y)$?

6. **(15 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 $13 \cdot x \equiv 1 \pmod{16}$ holds.

   (b) Without writing down the complete row from the multiplication table: does 4 have an inverse in $\mathbb{Z}_{170}$? Why (not)?

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