Homework 1: Concepts of Cryptography

Y. Desmedt

January 31, 2024

Due date: February 7, 2024 by 10:00am.

Students need to upload their answer to eLearning. Scanned handwritten homeworks are allowed provided the PDF file is less than 4 Mbytes.

Suggested Reading: https://en.wikipedia.org/wiki/Polynomial_long_division.

Recommendation: become familiar with software tools, such as Sage (free open software), or Gap (free software), or Mathematica (available at UTD: https://www.utdallas.edu/oit/howto/mathematica/). You can then generate as many problems you like similar to Problems 2 and 3 and test your knowledge!

Note: an exercise similar to one of the following problems, *will* be on Quiz 1. However, students will have *no access to a computer (or the like) during the quiz.*

Problem 1 Write the multiplication table for integers modulo 7. Moreover, use the table to find for each element its inverse, *if* it exists.

Problem 2 In AES $GF(2^8)$ is defined as an extension field of Z_2 by using the irreducible polynomial $x^8 + x^4 + x^3 + x + 1$. Now assume that $u \notin Z_2$ is a root of this polynomial. Perform the following multiplication:

$$u^7 * u^5 \bmod u^8 + u^4 + u^3 + u + 1 \bmod 2.$$

- Give the answer *without* using a computer program, write down your steps.
- Use Sage, Gap or Mathematica to verify the result. Print the output showing your steps. (A screenshot is fine too.)

Problem 3 Perform over $GF(2^8)$ using the same irreducible polynomial as in previous problem the following matrix multiplication:

$$\begin{pmatrix} u & 1 \\ u^2 & 1 \end{pmatrix} \cdot \begin{pmatrix} u^7 \\ u^6 \end{pmatrix}$$

- Give the answer *without* using a computer program, explain your steps.
- Use Sage, Gap or Mathematica to verify the result. Print the output showing your steps. (A screenshot is fine too.)