INSTITUTO POLITÉCNICO NACIONAL
ESCUELA SUPERIOR DE CÓMPUTO

Cryptography

Homework 1 *August 12th.*

1. Modular Arithmetic

Please do the following algorithms without a calculator. Solve them in a piece of paper, scan it and send it to me in a single file, next Tuesday 16th, before midday. The file must be a pdf and the filename must be as follows: Lastname_Name_modulararithmetic.pdf. For example: Diaz_Santiago_modulararithmetic.pdf

1. For each of the following exercises, give the result as an integer greater or equal than 0 and less than the module. For example $-3501 \text{ mód } 7 = 6$.
   a) $-81 \text{ mód } 7503$
   b) $-7503 \text{ mód } 81$
   c) $-100 \text{ mód } 24$
   d) $-5303 \text{ mód } 63$
   e) $-3 \text{ mód } 1111$
2. In the following exercises construct a multiplication table as we did it in class. Then see which elements have a multiplicative inverse. For example in $\mathbb{Z}_9$, 5 has multiplicative inverse:2, since $5 * 2 \text{ mód } 9 = 1$.
   a) $\mathbb{Z}_5$
   b) $\mathbb{Z}_8$
   c) $\mathbb{Z}_{11}$
   d) $\mathbb{Z}_{14}$
   e) $\mathbb{Z}_{13}$

   In general can you say when an element in $\mathbb{Z}_n$ has an inverse?
3. Find the integer x such that $5 * x \text{ mód } 13 = 1$
4. Find the integer x such that $5 * x \text{ mód } 7 = 1$
5. Compute $3 * 2/5 \text{ mód } 7$
6. Compute $(19 + 1/5) * 3 - 4/3 \text{ mód } 11$
7. Prove that $-a \text{ mód } m = m - (a \text{ mód } m)$

2. Classical encryption algorithms

For this section, you must send only one report for each team of 3 people , next Thursday 18th before midday. Please include your names in the report. The file must be a pdf and the filename must be as follows: Lastname_Name_classicalalgorithms.pdf. For example: Diaz_Santiago_classicalalgorithms.pdf.

1. Describe how to encrypt and decrypt using the following ciphers. Pay attention to the modular arithmetic involved in each of them.
   a) Vigenere cipher
   b) Hill cipher
   c) Affine cipher
2. Make your own example to encrypt and decrypt for each of the previous . Do not copy an example already done.
3. Determine how to break each of them.