INSTITUTO POLITÉCNICO NACIONAL
ESCUELA SUPERIOR DE CÓMPUTO

Cryptography

Homework 2

August 31st.

The following exercises are for training. You do not need to send the solutions, but if you have doubts or concerns, please contact me as soon as possible.

1. Which are the elements of each of the following groups:
   a) $\mathbb{Z}_{23}$
   b) $\mathbb{Z}_{23}^*$
   c) $\mathbb{Z}_{33}$
   d) $\mathbb{Z}_{33}^*$
   e) $\mathbb{Z}_{30}^*$
   f) $\mathbb{Z}_{30}$
2. List all the invertible elements in $\mathbb{Z}_m$, for $m = 28, 33$ and 35.
3. Determine the number of keys in an *Affine cipher* over $\mathbb{Z}_m$ for $m = 30, 100$ and 1225.
4. An obvious approach to increase the security of a symmetric algorithm is to apply the same cipher twice, i.e.:
   $$y = e_{k2}(e_{k1})$$
   As it is often the case in cryptography, things are very tricky and results are often different from the expected and/or desired ones. In this problem we show that a double encryption with affine cipher is only as secure as single encryption! Assume two affine ciphers $e_{k_1} = a_1x + b_1$ and $e_{k_2} = a_2x + b_2$.
   a) Show that there is a single affine cipher $e_{k_3} = a_3x + b_3$ which performs exactly the same encryption (and decryption) as the combination $e_{k2}(e_{k1})$.
   b) Find the values for a_3, b_3, when $a_1 = 3, b_1 = 5$ and $a_2 = 11, b_2 = 7$
   c) For verification encrypt the letter H first with e_{K1} and the result with e_{K2}. Then encrypt H with e_{k3}.
   d) Briefly describe what happens if an exhaustive key-search attack is applied to a double-encrypted affine ciphertext. Is the effective key space increased? Justify your answer.
5. Determine the inverses of the following matrices over $\mathbb{Z}_{26}$
   a) $\begin{pmatrix} 2 & 9 \\ 9 & 5 \end{pmatrix}$
   b) $\begin{pmatrix} 1 & 11 & 12 \\ 4 & 23 & 2 \\ 17 & 15 & 9 \end{pmatrix}$

6. Suppose we are told that the plaintext

   breathtaking

   yields the ciphertext

   RUPOTENTOIFV

   where the Hill cipher is used, but the size of the matrix is not specified. Find the encryption matrix.

7. Find the inverse permutation, for each of the following permutations.

   a)

x	1	2	3	4	5	6
$\pi(x)$	5	3	1	2	4	6

   b)

x	1	2	3	4	5	6	7
$\pi(x)$	7	1	6	2	5	3	4

   c)

x	1	2	3	4	5	6	7	8	9	10
$\pi(x)$	10	2	4	9	1	6	8	7	3	5

8. Encrypt the plaintext GOD REWARDS FOOLS, using the permutation

x	1	2	3	4	5
$\pi(x)$	2	3	4	5	1

9. Find the plaintext corresponding to the following ciphertext, knowing that it was encrypted using a permutation of length 4. Also find the inverse permutation.

   HNAOEYDMIINCUAEQRCEUQLUOOECNAULREALFICDCXAYD

10. Consider the English alphabet, and the shift cipher. Express the shift k, as a permutation of lenght 26.