CSCI 6331/4331 – Cryptography – Spring 2011
George Washington University

Homework I: 30 points
due 24 January, in class or on Blackboard by 6 pm.

Policy on collaboration: All examinations, papers, and other graded work products and assignments are to be completed in conformance with The George Washington University Code of Academic Integrity. You may *not* discuss HWs among yourselves. Each student is expected to work on his or her own HW out independently. You may only refer to your class notes, the text book, and to class material such as slides, notes and links provided on the course website. You may not refer to any other material while working on the homework.

Any violations will be treated as violations of the Code of Academic Integrity.

Submit all HW in grader's mailbox by 6 pm on due date, or in class, or in Blackboard by 6 pm.

Note that you will receive no credit without an explanation of your answer. Note also that you will be evaluated for your approach, and for the clarity of your exposition.

1. (6 points) Is there a key for the affine cipher with alphabet $\{A, B, C, ...Z\}$ that encrypts "NOT" as "AXE"? If not, explain why not. If so, find it.

2. Determine the number of:

a. (4 points) bit permutations of strings of length n

b. (3 points) circular right shifts of strings of length n

c. (3 points) one-to-one mappings $f : \Sigma^n \to \Sigma^n$

Note that the numbers above are exactly the number of keys in a cryptosystem that encrypts bit strings of length n by performing (a) bit permutations (b) circular right shifts and (c) one-to-one mappings.

3. (4 points) Find a one-to-one mapping $f : \Sigma^n \to \Sigma^n$ that is not a bit permutation.

4a. Consider the shift cipher, with $\mathcal{P} = \mathcal{C} = \mathcal{K} = \mathbb{Z}_m$ for **even** m. Answer the following:

(i) (1 point) How many keys are used by this cipher?

(ii) (2 points) Given a particular ciphertext (string of symbols) of length n, $c = c_1c_2...c_n \in \mathbb{Z}_m^n$, how many possible messages could this correspond to?

4b. Consider a slightly different encryption scheme for $\mathcal{P} = \mathcal{C} = \mathcal{K} = \mathbb{Z}_m$ for **even** m. The scheme works as follows. The encryption key consists of two even elements, $k_1, k_2, \in \mathbb{Z}_m$. A message p of length n is denoted $p = p_1 p_2 ... p_n$ where $p_i \in \mathbb{Z}_m$. The symbol p_i is encrypted as symbol c_i where $c_i = p_i + k_{b(p_i)} \; mod \; m$ where $b(p_i) = 2$ if p_i is even and $b(p_i) = 1$ if p_i is odd. That is, p_i is shifted by key k_2 if p_i is even, and by k_1 if p_i is odd. Answer the following:

(1 points) (i) How many keys $k = (k_1, k_2)$ are used for this cipher?

(2 points) (ii) Describe how ciphertext encrypted as above is decrypted using the key $k = (k_1, k_2)$.

(3 points) (iii) Given a particular ciphertext of length n, how many possible messages could this correspond to?

(1 point) (iv) Comparing your answer in 4b(ii) to that in 4a, explain whether there is a benefit to using the two keys of problem 4b, when compared to the single shift cipher key of problem 4a.

Acknowledgements: The problems are either from, or motivated by: *Introduction to Cryptography* by Johannes A. Buchman.