

CSCI 284/162 – Cryptography – Spring 2009
George Washington University

Homework I: 45 points

due 30 January, 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 TA's mailbox by 6 pm on due date.

1. If an encryption function e_K is identical to the decryption function d_K , then the key is said to be an involutory key.
 - a. (7 points) Find all involutory keys for the Affine Cipher over \mathbb{Z}_m , where $e_{a,b}(x) = ax + b \pmod m$.
 - b. (3 points) Find all involutory keys for the permutation cipher over \mathbb{Z}_m using blocks of 2 elements.
 - c. (3 points) Find all involutory keys for the permutation cipher over \mathbb{Z}_m using blocks of 3 elements.
 - d. (7 points) Derive a recursive expression for the number of involutory keys for a permutation cipher over \mathbb{Z}_m using blocks of n elements. Use this expression and the results of parts (b) and (c) to obtain the number of involutory keys for the permutation cipher over \mathbb{Z}_m using blocks of 4 elements.
2. (8 points) Suppose that $K = (5, 21)$ is a key in an Affine Cipher over \mathbb{Z}_{31} .
 - (a) Express the decryption function $d_K(y)$ in the form $d_K(y) = a_0y + b_0$, where $a_0, b_0 \in \mathbb{Z}_{31}$.
 - (b) Prove that $d_K(e_K(x)) = x \forall x \in \mathbb{Z}_{31}$.
3. (7 points) Is there a key for the affine cipher with alphabet $\{A, B, C, \dots, Z\}$ that encrypts "FIR" as "ONE"? If not, explain why. If so, find it.
4. (10 points) Find a one-to-one map of \mathbb{Z}_2^n onto itself – i.e. find an encryption on \mathbb{Z}_2^n – that is not an affine cipher. Show clearly why it is not an affine cipher.

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