

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

**Homework 4**  
due 13 March 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 independently on his or her own HW; you may not collaborate with others, you may not copy one another's assignments, even in part. 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.*

**If you submit your HW in Blackboard, name your files:**  
**CS284\_HW3\_LASTNAME\_FIRSTNAME.zip or .rar or**  
**CS162\_HW3\_LASTNAME\_FIRSTNAME.zip or .rar**

The following problems are either directly from the text by Stinson, or motivated by problems in it.

1. Given any Latin square of order  $n$ , define a related cryptosystem:  $\mathcal{P} = \mathcal{C} = \mathcal{K} = \{1, 2, \dots, n\}$ .  $e_K(j) = \mathcal{L}(K, j)$  where  $\mathcal{L}$  is the  $n \times n$  array defining the Latin Square. Prove that this cryptosystem achieves perfect secrecy provided that every key is used with equal probability.

2. (a) Prove that the Affine cipher over  $Z_m$  achieves perfect secrecy if every key is used with equal probability.

(b) More generally, suppose we are given a probability distribution  $Pr[a]$  on the set

$$\{a \in Z_m : \gcd(a, m) = 1\}$$

Prove that the Affine Cipher over  $Z_m$  achieves perfect secrecy if every key  $(a, b)$  is used with probability  $\frac{Pr[a]}{m}$ .

$$\text{Hint: } Pr[m|c] = \frac{Pr[c|m]Pr[m]}{\sum_m Pr[c|m]Pr[m]} = \frac{\sum_a Pr[k=(a,c-ma)]Pr[m]}{\sum_m \sum_a Pr[k=(a,c-ma)]Pr[m]}$$

3. Suppose a cryptosystem achieves perfect secrecy for a particular plaintext distribution. Prove that perfect secrecy is maintained for any plaintext distribution.

4. Prove that if a cryptosystem has perfect secrecy and  $|\mathcal{K}| = |\mathcal{C}| = |\mathcal{P}|$ , then every ciphertext is equally probable.