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

Homework 3
due 4 March, 6 pm, **on Blackboard**

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) while working on the homework, and not to any other material.

All code must run on your hobbes account. The TA will make no attempt to debug your code, or determine why it does not run. You will be graded on the correctness of your output, and the quality of your code: efficiency and documentation. There will be no exceptions.

Under no circumstances may code be copied from anywhere: classmates, the web, any other source

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

Submit all HW in Blackboard by 6 pm on due date. Name your files:
CS6331_HW3_LASTNAME_FIRSTNAME.rar or .zip or
CS4331_HW3_LASTNAME_FIRSTNAME.rar or .zip

Consider an S-box with 8-bit input and 8-bit output, such that

$$y = x + 171 \; mod \; 256$$

where y is the S-box output and x the S-box input. Your goal is to determine the *entire* bias table for this S-box and to identify the input-output masks that produce the top ten biases. Thus you need to provide a table listing as follows (the values provided are examples):

No.	Input Mask	Output Mask	Bias
1	01	01	$\frac{1}{2}$
2	F5	6A	$\frac{1}{16}$
3			
..	..	..	..
10			

You should submit, in addition either (a) code that computes the 256×256 bias table and finds the top ten values of bias, or (b) a complete theoretical examination of what the biases are for each possible input-output mask pair, and what the top ten values are.