CSCI 6331 - Cryptography - Spring 2011
The George Washington University

Homework 4

due 6:00 pm, 27 April, 2011

CS 4331 students may do this assignment for some extra credit. The amount of extra credit will be decided sometime later

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.

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_HW4_LASTNAME_FIRSTNAME.rar or .zip or
CS4331_HW4_LASTNAME_FIRSTNAME.rar or .zip
Archive the code with the report and name the compressed file similarly, with extensions .tar or .rar or .zip

The programming assignment may be written in C, C++ or Java only.

Using the code written in HW 2, and the S-box and permutation described below, write code for a linear cryptanalysis attack on the SPN cipher to determine *any eight bits* of the last round key.

For this attack, you will need to generate linear approximations of the S-box, determine which approximations you will use for the attack, determine the bias for the attack, guess how many P/C pairs you will need for the attack, generate them, and then use them to test the code.

The code should be accompanied by a report, which describes what you did, why, what the results were, and whether they were expected, that is, whether they make sense. This is an open-ended assignment. You will need to perform a number of tasks and take a number of decisions not described here.

The permutation is $y = x + 4 \; mod \; 32$ where x is the input position and y is the output position. That is, the bits are circular shifted four bits to the right. The S-box for input XY in hexadecimal notation is $f(X)f(Y)$ in hexadecimal notation where f is as follows:

Z	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
f(Z)	A	F	3	9	B	8	2	4	E	0	C	1	5	6	D	7