

CSCI 284 - Cryptography - Spring 2008
George Washington University

Homework 4

due 6:00 pm, 21 April, 2008

CS 162 students may do this assignment for some extra credit. The amount of extra credit will be decided sometime later

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 discuss HWs among yourselves, and work on them in groups. However, each student is expected to write his or her own HW out independently; you may not copy one another's assignments, even in part. You may not collaborate with others on the quizzes, midterm, or final.

You are expected to cite all your sources in any written work that is not closed book. Sources may be papers, books, web sites, discussions with others - faculty, friends, students. For example, if, in a group, one student has a major idea that leads to a solution to a HW problem, all other students in the group should cite this student.

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

PLEASE submit all HW on Blackboard only. Name your report:

CS284_HW3_LASTNAME_FIRSTNAME.doc or .pdf.

CS162_ExtraCredit_LASTNAME_FIRSTNAME.doc or .pdf.

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. 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, the quality of your code: efficiency and documentation, and the quality of your report. There will be no exceptions.

On no account may you use code written by anyone else, whether you acknowledge it or not.

Using the code written in HW 2, and the S-box and permutation of the sample input provided on the website, perform a linear cryptanalysis attack on the SPN cipher to determine *any four 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

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.