

CSCI 284 - Cryptography - Spring 2009
George Washington University

Homework 6: due 29 April, 2009

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.

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:

CS284_HW6_LASTNAME_FIRSTNAME.rar or .zip or

CS162_HW6_LASTNAME_FIRSTNAME.rar or .zip

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

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.

This problem is No. 6.9 in the text.

Decrypt the ElGamal ciphertext presented in Table 6.3 on page 278 in the text (sorry, you will have to key it in yourself, or use OCR). The parameters of the system are: $p = 31847$, $\alpha = 5$, $a = 7899$ and $\beta = 18074$. Use efficient exponentiation and efficient inversion *mod* p .

The numbers you obtain may be converted to the English alphabet. Three letters in the English alphabet are converted to numbers as follows: if the three letters are represented by numbers abc (for example, DOG is represented by 3 14 6), this corresponds to the value $a \times 26^2 + b \times 26 + c$; thus DOG corresponds to 2398, CAT to 1371 and ZZZ to 17575. You have to invert this process for your final step; that is, given the results of ElGamal decryption, convert each value to a base 26 representation, which is straightforward to convert to the alphabet.

You should submit a report that describes what you did and the solutions you obtained, as well as all your code.