

COSC 6397 Computer and Network Security

Computer Science Department, University of Houston, Instructor: Rakesh Verma

Spring 2008, Homework 1, Exercises 1-4 due Friday Feb. 15 at 11am in class

Keep an organized Excel log of the time spent on each problem, and turn it in as part of the zip archive.

1. Go to the web site <http://www.pgpi.org/>, download and install PGP 8.0 or better version of PGP. Try out the software and comment on the user interface and performance of the software. Page limit - 1 page.

2. Professor Hadrice and Stasistan were confronted with the following message:

IRIOO NEET NHM WR TS GEK

Professor Hadrice was able to solve it immediately but Professor Stasistan was puzzled. Can you help the poor professor by explaining to him the kind of cipher that was employed and the plaintext message? (trick question) Why do you think Professor Hadrice was able to solve it quickly but Stasistan was puzzled for a long time?

3. Consider a Feistel cipher composed of 16 rounds with block length 128 bits and key length 128 bits. Suppose that for a given k the key scheduling algorithm determines values for the first 8 round keys, k_1, \dots, k_8 and then sets $k_9 = k_8, k_{10} = k_7, \dots, k_{16} = k_1$. Suppose you have a ciphertext c . Explain how, with access to an encryption oracle, you can decrypt c and determine m using just a single oracle query. An encryption oracle is a device whose details are not known to you and that when given a plaintext returns the corresponding ciphertext.
4. (a) Calculate using repeated squaring method $7^{356} \bmod 26$. Show all steps. (b) Consult any number theory book and report any advances on modular exponentiation beyond what was discussed in class; page limit - 1 page.
5. Due Monday Feb. 18 at 5pm. Implement in one of C/C++/Java a program to implement the Vigenere cipher. The program should run in the Linux environment. It should take two command line inputs: keyword of up to 100 characters and an option bit. If the option bit is 0 the program reads a message from a file called message.txt and encrypts it with the ciphertext going to the file secret.txt. If the option bit is 1, the program should read the ciphertext from the file secret.txt, decrypt it into the file message.txt. Your program should not assume that both these files will always exist. The source program, executable, the log, and 3 encryption file pairs should be zipped together into one archive called XYZZZZ.zip and emailed to me (should be received by me before 5pm) where X is your first initial, Y is your last initial and the Z's are last four digits of your university ID. The executable should be called vigenere (note the lower case).

Academic Honesty Policy: No collaboration with anyone or anything in or outside the course is allowed on any homeworks, exams and programming assignments (yes, that excludes the internet as well) except if it is **explicitly allowed** on a problem. The *appropriate* help of the instructor and (if applicable) the TA is of course allowed and encouraged.