

COSC 6397 Computer and Network Security

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

Spring 2009, Homework 1, Exercises 1-4 due Mar. 2 at 1pm 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. Recall the Hill cipher from class. Mallory steals Alice's Hill cipher machine, which uses a 2×2 matrix $M \pmod{26}$. He uses a chosen plaintext attack and finds that the plaintext `ba` encrypts to `ID` and the plaintext `zz` encrypts to `GA`. What is the matrix M ?
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 $11^{2009} \pmod{29}$. 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 Wed. March 11 at 5pm. Implement in one of C/Java a program to (i) given a keyword, encrypt plaintext using the Playfair cipher and (ii) given ciphertext generated by the Playfair cipher, analyze it and find the key. Assume you have access to a large amount of ciphertext only. The program should run in the Linux environment. It should take one or two command line inputs: an option flag and an optional key. If the option flag is 0, then the key must be present on the command line, and the program reads a message from a file called `message.txt` and encrypts it using the Playfair method with the ciphertext going to the file `secret.txt`. If the option flag is 1, then the key must be present, and the program decrypts ciphertext from the file `secret.txt` and puts the plaintext in `message.txt`. If the option flag is 2, then the key is not present, and the program reads ciphertext from the file `secret.txt`, analyzes the ciphertext to find the key and prints it on the screen and then decrypts ciphertext 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.