

CSCI 283 and CSCI 172- Graduate and Undergraduate Computer Security - Fall 2005
George Washington University

Homework III

due 26 October, 6 pm.

30 marks

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 test and final.

You are expected to cite all your sources in any written work that is not closed book: 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 files:

CS283_HW1_LASTNAME_FIRSTNAME.doc or .pdf or

CS172_HW1_LASTNAME_FIRSTNAME.doc or .pdf

1. The following ciphertext has been encrypted with the substitution cipher. It is also available in a text file from the class website. The original plaintext is in the English language, spaces have been retained, but punctuation marks have not.

```
... resk vti gtqb fs vti rtiqb suyqhok ges wogihgotk sk ctigs o hwwifsb o rtiqb ls hyycthdeokz ges
yhggestk roge h dqshc obsh tn rev fv fsk rscs escs gehg ow ktg ges dhws lsdhiws o hf hlhkbtkokz
dcogodhq bigosw lv lsokz escs hkb lsdhiws o ehjs ntikb jscv qoggqs gehg fhmsw wskws ok geow
gestcv tn vtiew hltig joczok whdconodsw hkb hkdoskg ytsgcv o dhkktg ok zttb dtkwdoskds dtkgokis
o hf csdhqqokz geow fowwotk offsboghsgv
nctf bhk lctrk'w hkzsqw hkb bsftkw
```

Cryptanalyze it (i.e. determine the original plaintext and the key for the substitution cipher) as follows. The main body of your HW will be responses to the questions below with explanations if necessary. Plaintext will be denoted in capitals, and ciphertext in lower-case.

You must program steps (a)-(f), and, in an appendix to your HW, attach copies of all code as well as copies of all output. The TA will not look through output to find the answers, she will use output to check that you have correctly reported your answers in the main body of the HW.

- a. (3 marks) Create a table of each letter in the ciphertext and the corresponding occurrences.
- b. (2 marks) Sort this table, in descending order, by the number of occurrences.
- c. (1 mark) The letter that occurs most often in the ciphertext, i.e. the letter at the top of the sorted table, is most likely to correspond to "E" in the plaintext. What is it?
- d. (1 mark) To determine the plaintext corresponding to the next few letters in the sorted table, substitute "E" in the appropriate places in the ciphertext.
- e. (3 marks) Now, count digrams that begin with "E". Create a table of these digrams with their number of occurrences. Sort this table.
- f. (3 marks) Similarly, count digrams that end with "E". Create a table of these digrams with their number of occurrences. Sort this table.
- g. (5 marks) Using the tables from (b), (e) and (f), can you determine the plaintext for any more letters of the ciphertext? What would they be? What would the ciphertext look like with these plaintext letters substituted? (i.e. what would a partial decryption look like given what you know?).
- h. (3 marks) "THE" is the trigram that occurs most often in the English language. Does this help you determine any more letters? Again, if it does, substitute those letters into the ciphertext.
- i. (3 marks) Do any of the other frequently occurring digrams and trigrams in the English language help you determine any more letters? (You may do (h) and (i) repeatedly if necessary). Again, if they do, substitute those letters into the ciphertext.
- j. (6 marks) By looking at the partially-decrypted text, determine the entire plaintext message and the key to the substitution cipher. Present the key as a lookup table indexed by the plaintext letters.