

CSCI 283 - Computer Security I - Fall 2003
George Washington University

Homework II

due September 24 before class.

Use programming if necessary. Attach copies of all code

(25 marks) 1. Obtain the English plaintext for the following ciphertext by answering the questions below. Note that spaces are retained.

```

zl  l toqghewz wff o sjvwl hqunz gtl fgthdunuqld  qh fhr
hdjvwkts fteku h w ewld qmlqjthuftwd d dzrtd egqzsbxumtd
ltezlhsfry ewlzf yjw kbouindyrtxud zufurfqf d bu ewlz huffljzhrnf
zl  zdttytqorltyt kzg o lwkruwhtqwdkz uq lwt wuuuzl tznwhukz
zkjzw ww j hfvrwx erzwxw zl  tqqxjw dhruqze ewtuluz zw j wztzo
nztuqvz tdqu twktx vykdnzf efyww tuhyttzeqq dnhgzqzq qnwzttddb
efyot ofxwrzdt nukrztyu ktqt qugqnyhdkbxojvwtqwhdnoyb
dkqzjrwwofkruw tfqfwdrey wwmhofbrbtstmlnltx yudwkrur oono qf tw
suuqmh nqeyohk dgtbr hzz xwewly dbf u wqzrthwzl wzuqvtq fg u m q
qh z u  bsywb hfhfn ququvwbbwqz ty qemjvwvq ow iqzt z dwqwhhwz

```

- Steve Martin, "Pure Drivel"

a. Write a program to count the number of occurrences of each letter in the ciphertext, and to arrange the letters in decreasing order of frequency of occurrence.

Is this encrypted using only a permutation cipher? Why or why not?

b. If this were encrypted by a substitution cipher, what would be the ciphertext letter corresponding to the plaintext letter "E"? Why?

c. Is this encrypted using only a substitution cipher? Why or why not?

d. If this were encrypted with a substitution cipher followed by a permutation cipher of column length n , what would happen to digrams? Trigrams?

e. If this were encrypted with a substitution cipher followed by a permutation cipher, is the column length of the permutation cipher more likely to be 5 or 6? Why? (You may write programs to help you with this answer).

f. Assuming the message is encrypted using a substitution cipher followed by a permutation cipher, and using the more likely column length obtained in d, obtain the plaintext

corresponding to the above ciphertext. You may use any combination of programming and working by hand that you are comfortable with.

(10 marks) 2. Your teacher needs to create random IDs for each student in the class so as to be able to post grades in a public place yet maintain student privacy. Her goal is to ensure that the student can check his or her own grade, but that nobody may determine another person's grade.

She decides to use encryption. She encrypts each student's name in one of the following ways, and gives the student the ciphertext as his or her random ID. She then lists the student's grade next to the ciphertext corresponding to the student.

For each of the following, state why or why not its use would be appropriate for the problem. In particular, describe vulnerabilities and attacks and their expense to the attacker, and the expense of a secure method to the professor.

Assume that the professor's public key is known widely, that all private keys are well-protected and revealed only to persons mentioned, that the list of students in the class is publicly available, and that, in accordance with good security practice, the professor makes known the method she uses.

- a. Encrypting student names with her private key from her public/private key pair.
- b. Encrypting student names with her public key.
- c. Encrypting student names with a shift cipher, key unknown to anyone but her.
- d. Encrypting student names with a substitution cipher, key unknown to anyone but her.
- e. Encrypting student names with a private key block-cipher protocol, using a different private key for each student, and providing the student with their private key.
- f. Encrypting student names with a private key block-cipher protocol, using the same private key for each student, and not providing the key to any student.
- g. Which of the above methods allow for
 - i. a known plaintext attack?
 - ii. a known ciphertext attack?
 - iii. a chosen plaintext attack?
 - iv. a chosen ciphertext attack?

(5 marks) 3. Suppose there are n students in a class who want to send encrypted messages to one another.

a. Suppose they use private key encryption.

i How many keys would each student have to manage? Why?

ii. How many different keys would exist in the system? Why?

b. Suppose they use public key encryption. Answer i and ii above.