

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

**Homework I Solutions**

due September 10 before class

Your response to Question C cannot be handwritten; your other responses may be.

**(2 marks) A. Encrypt the following plaintext using the Caesar cipher with shift = 21:  
 CRYPTANALYSIS IS EASY**

Shift = 21 mod 26 is Shift = -5 mod 26.

ABCDEFGHIJKLMNOPQRSTUVWXYZ

vwxyzabcdefghijklmnopqrstu

xmtkovivgtndn dn zvnt

**(6 marks) B. Decrypt the following ciphertexts, encrypted using the Caesar cipher with unknown shift:**

1. **yjj rfc umpjb gq y qryec** There are only two single-lettered words in the English language, "A" and "I". If "y" is "A", then the decryption involves a shift of +2 mod 26, and the message decrypts to

ALL THE WORLD IS A STAGE

2. **This one is difficult. Try it once, then move on to the next question and come back later to this one.**

**kh cnn vjg yqtnf ygtg rcrgt cpf cnn vjg ugc ygtg kpm, kh cnn vjg vtgggu ygtg dtgcf cpf ejggug, yjcv yqwnf yg jcxg vq ftkpm?**

There is no single-lettered word, and the message is not quite long enough for a frequency analysis. One could try brute force, i.e. try each of the 26 possible keys. Or one could be slightly more intelligent. The question mark at the end implies the first word is either IS or IF, perhaps AS (this solution due to Anand Hemraj). If "k" decrypts to "I", the message decrypts to

IF ALL THE WORLD WERE PAPER AND ALL THE SEA WERE INK, IF ALL THE TREES WERE BREAD AND CHEESE, WHAT WOULD WE HAVE TO DRINK?

**(2 marks) C. Write one paragraph on why *you think* mathematics is or is not important in the study of computer security.**

There is no right or wrong answer here. All reasonable attempts will get full credit.