

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

**Homework I**

due September 10 before class

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

A. Encrypt the following plaintext using the Caesar cipher with shift = 21:

CRYPTANALYSIS IS EASY

B. Decrypt the following ciphertexts, encrypted using the Caesar cipher with unknown shift:

1. yjj rfc umpjb gq y qryec

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 vtggu ygtg dtgcf cpf ejggug, yjcv yqwnf yg jcxg vq ftkpm?

C. Write one paragraph on why *you think* mathematics is or is not important in the study of computer security. I do not expect you to read any other material to respond to this question, though you may wish to.

Among things you might want to - but do not have to - consider in your response are: what mathematics has brought to your understanding of other areas in computer science; what mathematics has made more difficult for you than simpler; what you think the study of security requires and why; what you think about the relationship between programming and the theory of computer science; how important implementation is vs. theory in security; how much you think mathematics might provide to the implementation of security. There is no right or wrong answer to this question. I simply want you to think through these questions and have an idea of what your opinion is, and what you do and do not know.

Your response may not exceed one printed page with reasonable margins; I hope it will be considerably less than that, about 20 lines (a little longer than this question).