COE 449: Network Security Engineering
HW 4 – Chapter 8
Posted: 17 November 2008 Due: 29 November 2008

1- Give your own example (real English sentence written by you) for simple substitution cipher where brute force attack will need 26! trails? Show how statistical frequency analysis can break it easily ?

2- Give your own example performing encryption using Vigenere Cipher assuming the key is three letters COE ? Show a real plaintext (understandable English words) scenario where it is very easy to break the system? Clarify your answer ?

3- Give your own simple example of transposition cipher and the cryptoanalysis method for breaking it? Show all your work of breaking this cryptosystem?

4- A cryptographer once stated that cryptography could provide complete security, and that any other computer security controls were unnecessary. Why is he wrong? (Hint: Think of an implementation of a cryptosystem, and ask yourself what aspect(s) of the implementation can cryptography not protect.)

5- Let *k* be the encipherment key for a Caesar cipher. The decipherment key differs; it is *26-k*. One of the characteristics of a public key system is that the encipherment and decipherment keys are different. Why then is the Caesar cipher a classical cryptosystem, not a public key cryptosystem? Be specific!!

6- Is the sum program, which exclusive or's all words in its input to generate a one-word output, a good cryptographic checksum function? Why or why not?

7- Propose your own hash function ? How can it resist collisions? Show an example of your work?

8- Explain through an example why the one time pad is an unconditional secure cryptosystem?

9- Give your example performing the RSA cryptosystem using numbers less than 100 ? Remember that you need to derive the keys first ?

10- Give an idea of public key cryptosystem not covered in the class ? show how encryption and decryption is performed ? Give a brief example to support your idea ?