CS 5352/6352 Computer Security

Homework 4

(30 pts)

1. Explain the three properties of one-way hash function.

2. What is a cryptosystem? Explain the five types of cryptanalytic attacks.

3. What is Rail Fence cipher? Convert the following plaintext into ciphertext using Rail Fence Cipher.

   ILOVECYBERSECURITY

4. Convert the following plaintext into ciphertext using Playfair Cipher.

   Key: MONARCHY
   Plaintext: INSTRUMENTS

5. Explain frequency attack on a substitution cipher.

6. Convert the following plaintext into ciphertext using Vernam Cipher (One-Time Pad).

   Key: HELLO
   Plaintext: WORLD

7. What is steganography? Mention some techniques of doing steganography.