

CS 167 — Fall 2006 — Goodrich — Midterm 1

Name:

ID:

1:

2:

3:

4:

5:

total:

1. (20 points). Please briefly answer each of the following short questions:

(a) What are the five parts that make up a *cryptosystem*?

(b) Briefly explain why any substitution cipher is not secure when it is applied to English text.

(c) Give an example of an affine cipher.

(d) What is a permutation cipher?

2. (20 points). Explain how encryption and decryption works in the one-time pad cryptosystem, and discuss why it achieves perfect security.

3. (20 points). Draw the data flow diagram (tracking how the bits move) in an example three-round Feistel Substitution-Permutation Network (SPN). Be sure to label all the constituent parts and briefly explain what they do.

4. (20 points). Explain how the electronic codebook (ECB) and cipher block chaining (CBC) modes work, and compare and contrast their relative strengths and weaknesses.

5. (20 points). Bob is stationed as a spy in Cyberia for a week and wants to prove every day of this week that he is alive and has not been captured. He has chosen a secret random number, x , which he memorized and told to no one. But he did tell his boss the value $y = h(h(h(h(h(h(h(x)))))))$, where h is a one-way function. Unfortunately, he knows that the Cyberian Intelligence Agency (CIA) was able to listen in on that message; hence, they also know the value of y . Explain how he can send a single message every day that proves he is still alive and has not been captured. Your solution should not allow anyone to replay any previous message from Bob as a (false) proof he is still alive.