Name: _____

Points: _____/100

Midterm Exam – Spring 2011, CSCI 530

1. **(3 pts)** Define what is vulnerability and what is exploit. What effect can exploit have on a system?

Vulnerability: Bug in software or misconfiguration that makes an application or OS behave in unexpected manner.

Exploit: Input/code that exercises the vulnerability

Effects: Crash the system, give attacker access (root or user level), slow down the system – pretty much any effect that the creator did not desire

2. **(5 pts)** Explain what is tragedy of commons. Why do we say that most problems in cyber security suffer from tragedy of commons phenomenon?

Def: Case when there's a shared resource and if a few people increase their use of resource they benefit but if everyone does that the resource gets depleted. Because most problems require solutions in places where people don't have economic incentive to solve them.

3. **(4 pts)** Describe how a homophonic cipher works. Then describe how a polymorphic (polyalphabetic) cipher works.

Homophonic: cipher symbols chosen randomly from a set. Frequency of symbol in plaintext determines size of set.

Polyalphabetic: Multiple mappings for symbols, one chosen for each symbol and then we advance to next mapping.

4. **(10 pts)** Define what is a block cipher and what is a stream cipher. What modes of operation exist for a block cipher (it is enough to just list the modes).

Block cipher maps groups of plaintext symbols (blocks) into sequences of cyphertext. Stream cipher maps each symbol into a symbol of cyphertext.

ECB, OFB, CFB, CBC

5. **(10 pts)** Explain how linear feedback shift registers work

- **Each step one bit is shifted out out of the register and becomes part of keystream**
- **One bit is added to the register by combining the bits that were there originally**
- **Primitive polynomials show us which bits to combine to cover the entire space of the register values**