Lecture 14 - Review

CSE543 - Fall 2006

Computer and Network Security

Professor Jaeger

October 24, 2006

Security Terminology

- Adversary
- Risks
- Vulnerability
- Threats
- Compromise
- Trust
- Trust Model
- Threat Model

Cryptography

- Encryption, Decryption
- Symmetric Key Systems
  - DES
  - One-time pads
- Public Key Systems
  - RSA
  - Diffie-Hellman
- Hash Functions
  - Uses
  - Properties
- Combinations of these into protocols
- Threats to crypto systems (use)