

# Study Questions

*"Computer Security"*

*Ch 12: Cryptography*

*Gollmann*

CS 4210 Advanced Operating Systems

Fall 1999 • Georgia Tech/Computer Science • Hutto

1. How is cryptography related to operating systems security?
2. Distributed systems introduce problems of message privacy, integrity and authentication. Briefly describe these three ideas and discuss how they are inter-related.
3. What is the key management problem? Why is it really difficult?
4. Briefly define the following terms and describe circumstances in which they might be used: digital signature, secure hash function, RSA encryption, DES encryption, certificate.
5. Briefly describe the Needham-Schroeder key establishment protocol. Is this a key agreement protocol or a key transport protocol? (What's the difference?)