Final Study Guide

This is simply a guide of topics that I consider important for the final. I don't promise to ask you about them all, or about any of these in particular; but I may very well ask you about any of these, as well as anything we discussed in class, in the discussion section, or that is in the readings (including the papers).

1. Everything contained in the midterm study guide
2. Confidentiality Models
   a. Bell-LaPadula Model
   b. Lattices and the BLP Model
   c. Tranquility
3. Integrity Models
   a. Biba Model
   b. Clark-Wilson model
4. Cryptography
   a. Types of attacks: ciphertext only, known plaintext, chosen plaintext
   b. Classical ciphers, Cæsar cipher, Vigenère cipher, one-time pad, AES
   c. Public key cryptosystems; RSA
   d. Confidentiality and authentication with secret key and public key systems
   e. Cryptographic hash functions
   f. Digital signatures
5. Key Distribution Protocols
   a. Kerberos and Needham-Schroeder
   b. Certificates and public key infrastructure
6. Authentication
   a. Passwords (selection, storage, attacks, aging)
   b. One-way hash functions (cryptographic hash functions)
   c. UNIX password scheme, what the salt is and its role
   d. Password selection, aging
   e. Challenge-response schemes
   f. EKE protocol
   g. Biometrics and other validation techniques
7. Identity and Anonymity
   a. Users, groups, and roles
   b. Identity in certificates
   c. Host identity (on the web)
   d. Web cookies
   e. Tor
   f. Cypherpunk, mixmaster remailers
8. Assurance
9. Electronic voting