

CS 331 Computer Networks

Network Security

- Encryption Methods
 - RSA
 - session key
 - Diffie-Hellman key exchange
- Authentication
 - Problem: Playback attack
 - Solution: nonce
 - security hole: man in the middle attack
- Message Integrity
 - hash function, message digest
- Cryptographic Hash Function
 - MD5
 - SHA-1
- Certificates
 - Solving the public key distribution problem
 - Trust is transitive
 - How is the initial trust established
 - Solution: Certificate Authority (CA)
 - Certificates - Issuance
 - Certificates - Use