CSC 479/579 WEEK 5 TEST STUDY GUIDE

GODFREY MUGANDA
DEPARTMENT OF COMPUTER SCIENCE
NORTH CENTRAL COLLEGE

In addition to the concepts on the week 4 quiz study guide, expect to be tested on the following concepts: operating modes for encryption, such as ECB, CBC, etc; generation of pseudo- random numbers, secure generation of pseudo-random numbers.

The number theory basis for the RSA and DH (Diffie-Hellman) cryptographic services: modular arithmetic, prime numbers, greatest common divisors and relatively prime numbers, multiplicative inverses, The Euler totient function $\phi(n)$, Fermat's Little Theorem, and Euler's Theorem. You should understand these theorems and be able to state them; generator or primitive roots modulo a prime.

Understand the process of generating a pair of keys for the RSA cryptosytem and why it is hard for an attacker to recover the private key if he or she knows the public key; understand the process of key agreement in Diffie-Hellman.

DSA and DSS (Digital Signature Algorithm)

Network security: vulnerabilities of broadcast networks, promiscuous mode of network adapters, packet sniffers, ARP and ARP spoofing attacks.