# CSC 479 WEEK 3 QUIZ

GODFREY MUGANDA

Here is a list of important topics and concepts for the week 3 Quiz:

Goals of security: confidentiality, integrity, availability, nonrepuadiation, non-forgeability.

Threats, attacks, vulnerabilities; denial of service, man in the middle attack; passive and active attackes; eavesdropping, masquerading, spoofing attacks.

Mechanisms used as tools to achieve security, such as encryption, authenticantion, authourization, access control; access control lists, access control matrix, capabilities.

Secret key encryption, public key encryption; advantanges and disadvantages of secret key and public key encryption, digital signatures, cryptographic hashes, one-way and collision-resistant functions; digital certificates; public key infrastructure; certificate authorities; message aunthentication codes, message integrity checks.

Probability of success in attacks on cryptography and digital signaturs when the plain text is a natural language; the birthday attack; ciphtertext-only, known plaintext, chosen plaintext, and chosen ciphertext attacks.