ITIS 6200/8200 Principles of Information Security and Privacy

Final Exam

If the questions ask for explanations, please **briefly** explain the **key reasons**.

Notation: here are some of techniques and notations that may be useful.

- AES: Enc(K, M) and Dec(K, C) where K, M, and C denote the key, plaintext, and ciphertext
- HMAC: HMAC(K, V) where K, V are the inputs to the HMAC function
- Hash: Hash(M) where M is the input to the hash function
- RSA: $E_{key}(M)$, and $D_{key}(C)$. The key here could be pub_[name], pri_[name] with the corresponding names. For example, $E_{pub\_alice}(M)$.
- c1 || c2: String concatenation of c1 and c2.