SE 4472 / ECE 9064 Midterm Solutions

Q1.

- (a) B
- (b) A
- (c) C
- (d) A
- (e) A
- (f) B
- (g) D
- (h) C **Note:** Question wasn't as clear as it could be, so I'm adding a mark to everyone's midterm in OWL.
- (i) A (See solution to Assignment 1, Question 2g)

Q2.

Ciphertext = 0148

Q3.

- (a) Hacker distributes malware with the same hash value and file name. To create a file that contains malware and produces the same hash, the hacker randomly modifies non essential portions of the file (e.g., text files, code comments, etc) until the desired hash value is achieved.
- (b) Second pre-image attack.
- (d) Due to a printing error there were two version of this question. If 4 characters then x = 4*4 = 16. If 6 characters then x = 4*6 = 24/

Q4.

- (a) Several strategies are possible, but the strategy in Assignment 1, Question 2 c) would also work in CTR mode.
- (b) No. The MAC portion of AES-GCM prevents A from generating valid ciphertexts,

and thus from making decryption queries based on modifying the challenge.