SE 4472 / ECE 9064 Sample midterm questions

1. (5 points) **Multiple Choice**. For each of the following questions, circle the best answer.

   (a) (1 point) Let c = {00, 01, 02, 03, 04, 05, 06, 07, 08, 09, 0A, 0B, 0C, 0D, 0E, 0F}. Is c a valid AES-256-ECB ciphertext?
   - A. Yes, always
   - B. No, never
   - C. It depends
   - D. Insufficient information to make a conclusion

   (b) (1 point) AES-GCM provides:
   - A. Confidentiality
   - B. Integrity
   - C. Authenticity
   - D. A. and B.
   - E. A. and C.
   - F. B. and C.
   - G. All of the above

   (c) (1 point) SHA-1 has a 160-bit hash length. How many bits of security does this imply?:
   - A. 80
   - B. 160
   - C. 320
   - D. 2^{80}
   - E. 2^{160}
   - F. 2^{320}

   (d) (1 point) In the *chosen ciphertext* (CCA1) attack game the adversary has the following powers:
   - A. Can make encryption queries before and after the challenge
   - B. Can make decryption queries before the challenge
   - C. Can make decryption queries after the challenge
   - D. A. and B.
   - E. A. and C.
   - F. B. and C.
   - G. All of the above

2. (2 points) Suppose you wished to encrypt the message “MIDTERM” using AES-256 with PKCS7 padding and UTF-8 encoding. Using the following UTF-8 encoding table, write the corresponding paintext in hexidecimal bytes.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
41	41	43	44	45	46	47	48	49	4A	4B	4C	4D	4E	4F	50	51	52	53	54	55	56	57	58	59	5A

3. (2 points) Let $E()$ be an encryption function that accepts a message and outputs a ciphertext c, consisting of the bits of m in shuffled order. Suppose the shuffle applied to m is determined by a highly non-linear function of the key k. Is $E()$ secure under any formal security notion studied in this course? Justify your answer.

4. (5 points) Consider the *Nibble Cipher*, a block cipher with a 4-bit block (a *nibble* is half a byte, or one hex character). Let ciphertext `9C25` be the encryption of a message using the Nibble Cipher in CBC mode with an IV of `B`.

   Using Table 1 on the **following page**, decrypt the ciphertext to recover the message. For your convenience, Table 2 lists the xor of all possible nibble pairs.

Tables for question 3

c	$m = \mathsf{Dec}_k(c)$
0	9
1	6
2	2
3	A
4	B
5	D
6	F
7	C
8	E
9	0
A	3
B	5
C	7
D	1
E	8
F	4

Table 1: Nibble cipher decryption table

		y															
		0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
x	0	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
	1	1	0	3	2	5	4	7	6	9	8	B	A	D	C	F	E
	2	2	3	0	1	6	7	4	5	A	B	8	9	E	F	C	D
	3	3	2	1	0	7	6	5	4	B	A	9	8	F	E	D	C
	4	4	5	6	7	0	1	2	3	C	D	E	F	8	9	A	B
	5	5	4	7	6	1	0	3	2	D	C	F	E	9	8	B	A
	6	6	7	4	5	2	3	0	1	E	F	C	D	A	B	8	9
	7	7	6	5	4	3	2	1	0	F	E	D	C	B	A	9	8
	8	8	9	A	B	C	D	E	F	0	1	2	3	4	5	6	7
	9	9	8	B	A	D	C	F	E	1	0	3	2	5	4	7	6
	A	A	B	8	9	E	F	C	D	2	3	0	1	6	7	4	5
	B	B	A	9	8	F	E	D	C	3	2	1	0	7	6	5	4
	C	C	D	E	F	8	9	A	B	4	5	6	7	0	1	2	3
	D	D	C	F	E	9	8	B	A	5	4	7	6	1	0	3	2
	E	E	F	C	D	A	B	8	9	6	7	4	5	2	3	0	1
	F	F	E	D	C	B	A	9	8	7	6	5	4	3	2	1	0

Table 2: Xor lookup table ($x \oplus y$)

5. (4 points) **Security games**.

   (a) (3 points) Consider AES in counter mode (AES-CTR). Give a strategy that would allow an adversary to win the CCA2 game with advantage.