CSC 4222/6222 – Exam #3 **Name: ______________________________**
Spring 2020

This exam is open book and open notes, but **closed partner**. You must **justify your answers and/or show your work**, without this, you will not receive any credit. State any assumptions needed. Make sure to submit your written work by 10:30 am to the dropbox folder. Ensure that any files submitted are legible. Ideally, you will be submitting one pdf file of all your work. Do not forget to write your name on the top of the first page and provide a signature corresponding to the statement below – and clearly number your problems.

In accordance with both the letter and spirit of the University Policy on Academic Honesty, I have neither given nor received assistance on this examination.

SIGNATURE: ______________________________

1. Consider using the ECB block cipher so that the secret key K is chained as follows:

$$C[i] = E_K(C[i-1] \oplus P[i]) \quad and$$
$$P[i] = D_K(C[i] \oplus C[i-1])$$

Where $C[-1]$ is the initialization vector and K is the secret key known to both transmitter and receiver. E_K and D_K represent the encryption and decryption, respectively. Suppose that ciphertext $C[7]$ is damaged in transmission. Will this impact being able to decipher any of the plaintext blocks, $P[i]$? If so, explain which one(s) and why. If not, explain why not. [10 points]

2. Assume Alice and Bob are using the Diffie-Hellman key exchange protocol to establish a shared secret key for a **Ceasar cipher**. The public parameters used are p=23 and g=9. Bob's picks a random positive number y=6 for his exponent value to compute Y and then sends Y to Alice, while Alice has sent X=16 to Bob. At this point, both Alice and Bob have been able to compute the shared secret key. Show your work. [15 points] (Parts a & b)

    a. What is the secret key?

    b. If Bob wants to send plaintext = "HEY", what would the encrypted text be?

3. Assume the plaintext has been transformed to the following state array as shown below within one of the rounds of the AES encryption scheme. This state is now being fed to the SubBytes step and then the output of that will be fed to the ShiftRows step. Show the output of the two steps for the one row left blank. [20 points]

Current State

5A	26	0A	19
1B	40	9C	3A
9F	1C	7E	39
C2	06	4B	27

xx	xx	xx	xx
xx	xx	xx	xx
xx	xx	xx	xx

After SubBytes

xx	xx	xx	xx
xx	xx	xx	xx
xx	xx	xx	xx

After ShiftRows

Now, using the **“<u>Current State</u>”** matrix as input, calculate the resulting value for cell [0,1] after the MixColumns step. Show your work.

4. Alice and Bob are using RSA to communicate. Alice's public encryption key is (n, e) = (253, 13) and her private key is d = 17. Bob wants to encrypt the plaintext message of value 5 to send to Alice. What is the ciphertext that he sends? Show the steps. [10 points]

5. Short computation problems. Make sure to use any indicated method to receive full credit. (Parts a-c) [20 points]

   a. Compute *gcd* (6573, 54) using Euclid's GCD algorithm. Show all your steps.

   b. Determine if residue element 84 of $\mathbb{Z}_{497}$ has a multiplicative inverse. Show your work to justify your answer.

   c. Compute the multiplicative inverse of residue element 47 in Z_{93}. Use the Extended Euclidean algorithm to show your work. If there is no inverse, explain why.

6. More short problems. Justify all answers. (Parts a – d). [25 points]

   a. Determine the totient function of 27, $\phi(27)$. Justify your answer.

   b. Determine how many generators there are for $n = 31$. Justify your answer.

   c. Find the inverse of 6, where $6 \in Z_{13}$. Do NOT use the Extended Euclidean algorithm or an online inverse tool. Justify your answer using the properties/theorems we discussed.

   d. Compute $4^{37} mod\ 21$ using Repeated Squaring to show your work.

Matrix to use for the AES MixColumns Transformation calculation:

$$\begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix}$$

	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
1	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
2	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
3	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
4	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
5	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
6	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
7	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
8	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
9	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
a	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
b	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
c	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
d	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
e	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
f	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

Figure 8.14: The S-box used in the SubBytes step of AES. Each byte is shown in hexadecimal notation, which encodes each 4-bit string as a digit 0–9 or a–f. Each byte is indexed according to the first and second 4-bits in the byte to be transformed.