CS458-01/02/03 - Spring 2020
Problem Set 2
Due in Blackboard on Monday, March 2nd by Midnight (11:59pm)

Problem 1

We now consider the relation between passwords and key size. For this purpose we consider a cryptosystem where the user enters a key in the form of a password.

a. Assume a password consisting of 8 letters, where each letter is encoded by the ASCII scheme (7 bits per character, i.e., 128 possible characters). What is the size of the key space which can be constructed by such passwords?

b. What is the corresponding key length in bits?

c. Assume that most users use only the 26 lowercase letters from the alphabet instead of the full 7 bits of the ASCII-encoding. What is the corresponding key length in bits in this case?

Problem 2

One important property which makes DES secure is that the *S-boxes* are nonlinear. How would you **verify** (not prove of course) the non-linearity of *S-box 1* of DES using the following input pairs

1. x_1 = 000000, x_2 = 000001
2. x_1 = 111111, x_2 = 100000

S-Box 1 of DES

	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**
0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
2	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

Problem 3

Explain the self-healing property of cipher block chaining mode?

Problem 4

Perform encryption using the RSA algorithm, for the following:

1. *p = 3, q = 11, e = 7, M = 5*
2. *p = 5, q = 17, e = 3, M = 9*

Problem 5

Perform decryption using the RSA algorithm, for *p = 11, q = 13, e = 11; C = 106*

Problem 6

In a public-key system using RSA, you intercept the ciphertext *C =10* sent to a user whose public key is *e=5*, *n=35*. What is the plaintext *M*?

Problem 7

Alice and Bob use the Diffie-Hellman key exchange technique with a common prime $p = 71$ and a primitive root $\alpha = 7$.

1. If Alice has private key $k_{pr,A} = 5$, what is Alice's public key $k_{pub,A}$?
2. If Bob has private key $k_{pr,B} = 12$, what is Bob's public key $k_{pub,B}$?
3. What is the shared secret key?