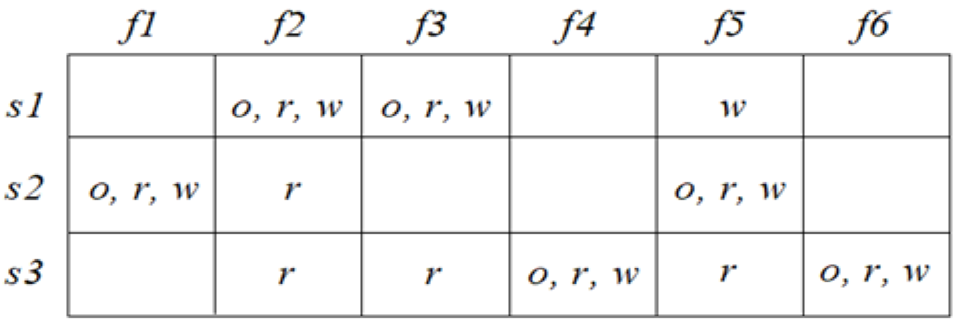
San Diego State University
CS574 Computer Security
Homework Assignment #3
Due: March 31, 2020 11:59 PM

● Please type the solutions using a word processor such as MS Word, Latex, or write by hand neatly and upload the scanned copy of it.

● I, _______________ (sign your name here), guarantee that this homework is my independent work and I have never copied any part from other resources. Also, I acknowledge and agree with the plagiarism penalty specified in the course syllabus.

● Turn in your assignment through the blackboard before the deadline. Penalty will be applied to late submission.

1. (10 points) For the given Access matrix below:
   a. Draw access control lists for s1, s2 and s3
   b. Draw capability lists for s1, s2 and s3



	f1	*f2*	*f3*	*f4*	*f5*	*f6*
s1		*o, r, w*	*o, r, w*		*w*	
s2	*o, r, w*	*r*			*o, r, w*	
s3		*r*	*r*	*o, r, w*	*r*	*o, r, w*

2. (12 points) Which of these is an example capability system, and which is an ACL-based approach?

   a. A wedding ceremony has a list of invited guests.
   b. Your office has card-swipe access, where the magnetic code on the card is matched against a list of employees.
   c. You give your car keys to your roommate.
   d. Your car has a parking permit specifying where you're allowed to park.

3. (10 points) Capabilities could be described as an authorization mechanism that is based on “something you have”. How might we analogously describe the following mechanisms for controlling access to confidential information?

   a. Access control lists.
   b. Encryption.

4. (10 Points)

a. Suggest a way of implementing protection domains using access control lists.
b. Suggest a way of implementing protection domains using capability tickets.

5. (14 points) Discuss the strengths and weaknesses of implementing an access matrix using capabilities that are associated with domains.

6. (14 Points) A secure biometrics system authenticates the user based on his/her physiological (e.g., fingerprint, face, voice) or behavioral (e.g., gait, hand gesture, keystroke) traits. Typically, a binary classification model will be developed to generate predicted probabilities based on the input information. Please explain:

a. How do you convert the predicted probabilities into class predictions?
b. How do you generate the ROC curve when you want to evaluate your system performance?

7. (10 Points) A security company proposes the following authentication scheme using a hash function: the client and the server both maintain a secret string, which is initialized to some 16-word random value. Whenever the client wants to authenticate itself, the server will generate a random challenge r, of length 16 words, and send it to the client. The client replies $h(s \,||\, r)$ and the server will verify its value. If it is a match, both sides will update s by appending r to it (i.e., $s \leftarrow s \,||\, r$). Otherwise, the server rejects the client and leaves s unchanged. After a cursory look, an experienced attacker says:" They'd better not to use MD family. Its only good if h is a random oracle."

a. (8 points) Explain why an MD family like MD4 or MD5 is not a good candidate. You may ignore the padding.
b. (2 points) Explain why a RO is secure.

8. (20 Points) You are in an undercover operation at a secret agency and your mission is to collect intelligence.

One day, you hear the following conversation when the supervisor assigns a mission. "Normally, I won't assign it to a rookie," the supervisor talks to Tom, "but we are short-handed and there are several confidential messages we need to send to the client."

"Do we need to encrypt it?" he asks.

The supervisor looks at him in disbelief. "Didn't Chen teach you the meaning of confidential?"

He stares blankly at the supervisor, "He forgot…but maybe we can try …-time-pad?"

"Make yourself useful and get it done asap!" the supervisor leaves furiously.

Tom is scared and couldn't stop mumbling:" okay…okay…I can do this. But is it one-time-pad or two-time-pad?"

You seize the opportunity and quickly approach him, pretending that you just walk by: "Hey, Tom. You look great today. Are you just talking about one-time-pad and two-time-pad? Hey easy, they are nothing different and all secure. Actually, encrypting two with one pad makes things quicker."

"Oh, thank you. You are really my life-saver!" Tom looks at you admiringly.

You say goodbye to Tom and run back to your desk. Eventually, you intercept 4 ciphertexts (refer to the attached *HW3_twotimepad.txt*). After discussing with the boss, you have the following information:

1. You are pretty confident that Tom encrypts these 4 messages using only 2 secret keys. In other words, 2 messages are padded (XOR) with the same secret key.
2. Your boss tells you that the messages are most likely encoded with the ASCII system and you decide to look into ASCII 32-127 first.
3. You suspect that one message is a piece of C++ code, one message says something about the CS574 midterm exam, one message includes many prime numbers, and the last message contains some famous movie dialogue.

Your job is to explain your approach and implement a python program to:

a. Find the pairs. **Hint**: Assume the plaintexts are in (non-extended) ASCII code, you know that the first bit in each byte is always 0. Think about the property of XOR.
b. Decrypt 4 messages and you need a good strategy and of course, some luck. **Hint**: $C_1 \oplus C_2 = (M_1 \oplus K) \oplus (M_2 \oplus K) = M_1 \oplus M_2$

It's okay if you make few mistakes. Your approach is always more important than the absolute result.