**San Diego State University**

**CS574 Computer Security**

**Homework Assignment #3**

**Due:**

● 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.

1. (10 points) For given Access matrix below:
2. Draw access control lists for files. (f1, f2, ..., f6)
3. Draw capability list for files. (s1, s2, s3)

A picture containing text, sky, light

Description automatically generated

1. (10 Points) Which of these is an example capability system, and which is an ACL-based approach?
   1. A wedding ceremony has a list of invited guests.
   2. Your office has card-swipe access, where the magnetic code on the card is matched against a list of employees.
   3. You give your friend a key to your apartment
   4. Your car has a parking permit specifying where you're allowed to park.
2. (15 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:
   1. How do you convert the predicted probabilities into class predictions?
   2. How do you generate the ROC curve when you want to evaluate your system Performance?
3. (15 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 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 ⇠). 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 good if is a random oracle.”
   1. (10 Points) Explain why an MD family like MD4 or MD5 is not a good candidate. You may ignore the padding.
   2. (5 Points) Explain why a RO is secure.
4. (20 Points) Perform a lab on ACLs on any Ubuntu machine. For each step, attach a screenshot of your operation. Follow the below steps:
5. (5 points) Create a new file sample.txt and list its permission using ‘ls’ command. Change the permissions of the file using the ‘chmod’ command. What’s the problem when we use chmod command. How does ACL help overcome this problem?
6. (5 points) By default, ACL package should be part of your Ubuntu system. If ACL is not installed, use following command to do so:

**$sudo apt install acl**

To verify if ACL package is installed on your system, you can use following command:

Graphical user interface

Description automatically generated

You should get a similar output as shown below if it is already installed.

Graphical user interface

Description automatically generated

Display the file permissions of sample.txt using the command from ACL package. Assign read, write and execute permissions to the sample.txt file for any group of your choosing (You can create new group or assign to an existing one). Verify the permissions by displaying them.

1. (4 points) Create a new user “tom”. Grant read only permissions to tom for the sample.txt file. Display the permissions.
2. (3 points) Create another file test.txt. Copy the ACL’s from sample.txt to test.txt using a single command. Verify the permission’s by displaying them.
3. (3 points) Remove all the assigned ACL’s from sample.txt and revert to default ACL’s (as in when the file was created). Display the final permission’s of sample.txt.
4. (30 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 is not that good…but maybe we can try …-time-pad?”

“Finally, make yourself useful and get it done asap!” the supervisor leaves furiously.

Tom is still 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 thinking 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 the attached HW3\_TwoPadAttack.docx. After discussing with your boss, you have the following information:

1. You are 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 investigate ASCII 32-127 first.
3. You suspect that one message is a piece of C code, one message says something about CS574, one message includes many prime numbers, and the last message contains some song lyrics.

You job is to explain your approach and implement the program to:

* 1. Find the key pairs. Hint: Assume the plaintexts are in (non-extended) ASCII code, then you know that the first bit in each byte is always 0. Think about the property of XOR.
  2. Decrypt 4 messages and you need a good strategy and of course, some luck.

Hint: