**USC UPSTATE**

**CSCI 455: Computer Security**

**Spring 2019**

**Homework Assignment 4**

**Problem 1**

Suppose that you want to share a secret file with three users, however you want them to be able to open the file *only when* all three of them are present. Describe a method to encrypt a file to the three users so that they are able to decrypt the file *only when* all three are present, that is, they would not be able to decrypt file if just one of the three users is absent. Explain why your method works. Also describe how the three users would decrypt and open the file when they are all present.

Split the key into three different sections and give each member a different section. Then each user has a part of the decryption key. The file then cannot be decrypted by any single or double pairing of users since they wouldn’t have the whole key. All three users would have to come together and supply their section of the key to decrypt the file.

**Problem 2**

Recall that an encryption scheme is said to be *deterministic* if under the same encryption key, every message has a *unique* ciphertext. That is, when the key is fixed, every time a message is encrypted the resulting ciphertext is the same.

1. Suppose that in a given situation there are only *3 possible messages that are publicly known* (for instance, think of a presidential election where there are 3 candidates), and a *deterministic* *public-key* encryption scheme is employed to encrypt messages. Describe a method by which an attacker can determine, in this situation, the plaintext of any intercepted ciphertext produced by a known public encryption key, *without* the matching private decryption key. Justify your answer. (**Note**: The answer to this question implies that a secure public-key encryption scheme must be *probabilistic*, that is, every message must have many possible ciphertexts even under the same encryption key.)

To figure out with message goes with which ciphertext, an attacker can encrypt each plaintext message with the known public key. Since the message is a deterministic scheme, encrypting the plaintext will yield one of the 3 ciphertexts. Then comparing each ciphertext, an attacker can tell which is which.

1. How would your answer in Part (a) change if a deterministic *private-key* encryption scheme is used instead? Justify your answer.

If each original message is encrypted with the private-key first, then an attacker can decrypt the messages using the known public key. Doing this an attacker can compare the plaintexts to find which one the original ciphertext goes with.