# HW2

Name: Gengda Li

## Part 1 (5Pts): Symmetric Key Encryption Modes

Use the SDES calculator provided in the blackboard site to perform the following encryptions using the specified mode. Here is an example question and its answer (please follow the same format for answering):

*Encrypt 10101010010111111010101001011111 using the key 1011001101 in codebook mode. Identify the blocks of plaintext?*  
*Blocks of plaintext:*

* *b1: 10101010*
* *b2: 01011111*
* *b3: 10101010*
* *b4: 01011111*

*Ciphertext: 00110001100111010011000110011101*

1. (2pts) Encrypt 10101010 01111111 10101010 11111111 using the key 1010101010 in electronic codebook mode.
   1. Identify the blocks of plaintext?

b1: 10101010

b2: 01111111

b3: 10101010

b4: 11111111

* 1. What is the ciphertext?

01101011 10101010 01101011 00001000

* 1. How many bits are different between plaintext blocks 1 and 3? How many bits are different between their corresponding ciphertext blocks?

The answers of these two questions are same: 0 bit is different.

* 1. How many bits are different between plaintext blocks 2 and 4? How many bits are different between their corresponding ciphertext blocks? (recall the concept of “changing one bit in plaintext changes ciphertext by half” that we talked about in class).
     + 1. 1 bit is different
       2. 3 bits are different

1. (1.5pts) Encrypt 10101010 01111111 10101010 11111111 using the key 1010101010 in CBC mode. Use IV 11000011. Use the symbol ⊕ for XOR. The calculator won’t do the XOR for you. You have to do it manually.
   1. What is the ciphertext?

10000111 10000010 01101110 10100110

* 1. How many bits are different between plaintext blocks 1 and 3? How many bits are different between their corresponding ciphertext blocks now?

(1)0 bit is different

(2)5 bits are different

1. (1.5pts) Decrypt 10101010 01111111 10101010 11111111 using the key 1010101010 in counter mode. Assume the counter starts at 0 (i.e. 00000000, 00000001, and so on). Use the symbol ⊕ for XOR.
   1. What is the plaintext?

10010000 11101010 11100001 10101001

* 1. If you were asked to encrypt the message (rather than decrypt it), will your answer in part (a) change? Why?

No, I do not need to change the answer. Because according to the data flow of the counter mode, if I want to decrypt message, the key and (counter+N-1) come into the encryption algorithm and the result XOR with the corresponding ciphertext block to get the plaintext. In encryption mode, the key and (counter+N-1) come into encryption algorithm and the result XOR with plaintext to get the cipher text. Because the text is same, so the answer is the same.

## Part2 (5pts): Hashing

Using the hash calculator at <http://www.fileformat.info/tool/hash.htm>, answer the following question:

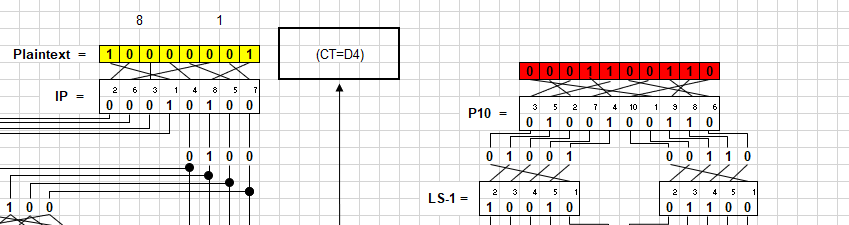
Consider the following **Hex** message: F2. This message was sent from Bob to Alice. Along with the message, Alice received from Bob a MAC: 2BA3119C (represented in Hex as well). The MAC was calculated using the mechanism described in figure 2.5a in the book. The encryption mechanism used was the simplified DES in ECB mode and key 0001100110. The hash function used was CRC32. Is the signature of the message correct? Describe your steps clearly (use bullets to describe steps).

STEP 1:

Get the CRC32 message of “F2”, is 81b17cbd

STEP 2:

Take the “81b17cbd” as the plaintext input, use the key 0001100110 as the key, to get the DES in ECB mode results.



Then we can get the final message “d436fb18”.

STEP 3:

Get the CRC32 message of MAC “2BA3119C”, is dfb47955.

STEP 4:

Combine the Hex message “F2” and the DES result “d436fb18” into one new message “F2D436FB18”. And get the CRC32 message “0ea363d5”.

STEP 5: Because the results of STEP 4 and STEP 5 are different, so it is uncorrect.

## Part3 (5pts): Password Cracking

Using “John the Ripper”, which is available in Kali, break the Linux shadow (password) file included with this assignment for users “root” , “john”, and “hackmeifyoucan”. You will need some dictionary files, which is also included. Describe how you broke the passwords and show a screen shot of the cracked password.

Explain the meaning of each field on both the password and shadow files. What are the differences between the different shells assigned to each user?

Which users are actually allowed to login from the console on the machine where this file resides (hint: look at the shells assigned to each account in the passwd file and what they mean)?

Part 1: Use the “John the Ripper” to crack password.

* 1. install

sudo apt-get install john

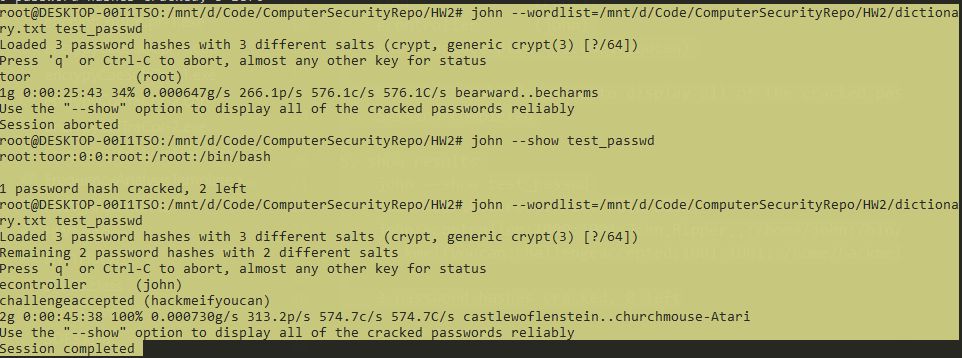
* 1. combine files

unshadow passwd shadow > test\_passwd

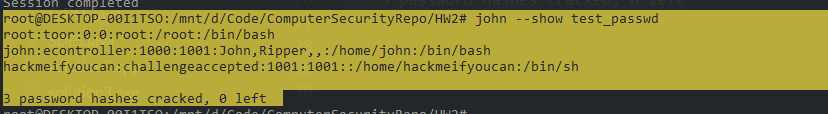
* 1. use dictionary crack password

john --wordlist=/mnt/d/Code/ComputerSecurityRepo/HW2/dictionary.txt test\_passwd

* 1. wait for results



* 1. show results



The passwords are:

root:toor:0:0:root:/root:/bin/bash

john:econtroller:1000:1001:John,Ripper,,:/home/john:/bin/bash

hackmeifyoucan:challengeaccepted:1001:1001::/home/hackmeifyoucan:/bin/sh

Part 2:

The /etc/shadow file stores actual password in encrypted format (more like the hash of the password) for user’s account with additional properties related to user password. Basically, it stores secure user account information.

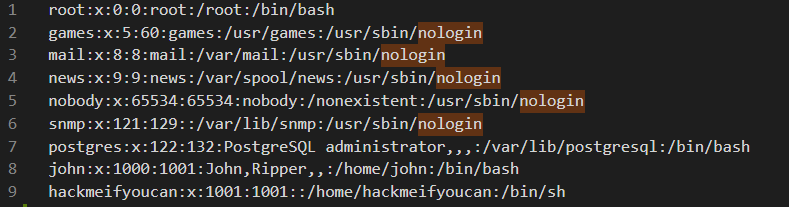
/etc/passwd file stores essential information, which required during login. In other words, it stores user account information. The /etc/passwd is a plain text file. It contains a list of the system’s accounts, giving for each account some useful information like user ID, group ID, home directory, shell, and more. The /etc/passwd file should have general read permission as many command utilities use it to map user IDs to user names. However, write access to the /etc/passwd must only limit for the superuser/root account.

The differences:

passwd is the file where the user information (like username, user ID, group ID, location of home directory, login shell, ...) is stored when a new user is created.shadow is the file where important information (like an encrypted form of the password of a user, the day the password expires, whether or not the passwd has to be changed, the minimum and maximum time between password changes, ...) is stored when a new user is created.

Part 3:

This is the passwd file:



We can see that there are some users are “nologin”. So the remain users can login from the console.

They are root, postgres, john, and hackmeifyoucan.

Reference

All the information and the HW2 notes are uploaded to my GitHub Repo.

<https://github.com/SaberDa/ComputerSecurityRepo/tree/master/HW2>