COMP 189: Homework #7

Assigned Mar 11, 2022
Due Mar 18, 2022

48 points total

Instructions: *For each problem, show all your work (required for credit). For answers requiring written answers, use no more than 4 sentences.*
Submission Instructions: *submit your solutions in PDF format through MyCourses Assignments.*

Technical Exercises

1. Security Database (10 pts)

Netflix follows industry security standards and stores all their users' authentication information in a table called *User*.

1. Write out the schema for this table – there are 3 fields in particular that must appear.

User
- id: bigint not null pk
- username: varchar(50) not null
- password: varchar(50) not null

2. A hacker has gained access to this database. Give the query she will write to obtain all authentication information for users.

```
SELECT username, password FROM user;
```

3. Even once the hacker has downloaded all the data – why isn't she able to log in as one of the user's right away.

This is because the passwords are hashed. The hacker would need to decrypt the hashed password to be then able to login, which is not possible.

2. Password complexity (8 pts)

Calculate the number of valid passwords implied by a length 6 password that satisfies the following password rules.

Scheme 1:
- Capital and lowercase letters

There are a total of 26 letters in the alphabet. Multiplied by two because of lower and upper case which is 52. And there at 6 different characters. Hence:

(26*2)^6 = 52^6 = 19,770,609,664 possible passwords

Scheme 2:
- Capital and lowercase letters
- At least one character is a number

Like above there are 26 x 2 possible letters and 10 digits to choose from (0 to 9). Meaning there are 52 + 10 = 62 possible selections for each slot in the password. We need AT LEAST

one digit in the password. The total number of passwords with letters and digits is 62^6. Now we remove the passwords with no digits from that number being 52^6. Hence:

62^6 – 52^6 = 37029625920 passwords with at least one digit

Scheme 3:

- Capital and lowercase letters
- At least one character is a number
- At least one character is a symbol (just those above the number keys)

Note that we have 10 extra symbols above the number keys from 0 to 9. 10 numbers, and 52 letters (lower case and upper case).

Similarly, to above. We have 52 + 10 + 10 = 72 possible characters for each slot in the password.
The total number of passwords is 72^6.
Passwords with no symbol but at least one digit = 62^6 – 52^6
Passwords with no digits but at least one symbol = 62^6 – 52^6
Passwords with no digits and no symbols = 52^6
Overall:

(62^6 – 52^6) + (62^6 – 52^6) + (52^6) passwords not allowed
➔ 72^6 – ((62^6 – 52^6) + (62^6 – 52^6) - (52^6)) = 85025427328 passwords with at least one digit and one symbol

3. Caesar Cypher (12 pts)

In class, we learned the notation Ecc(M,K) for encryption by Caesar cypher and Dcc(X,K) for decryption by Caesar cypher.

1. Compute Ecc(M, K) for M = “COMP189” with K = 3 (numbers precede letters when calculating the shifts)

The order or the cypher is like so:
➔ 0 1 2 3 4 5 6 7 8 9 A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Thus:
Ecc(“COMP189”, 3) = FRPS4BC

2. In #1, we used a key with a positive number… what is the equivalent key as a negative integer (i.e., a positive integer that has the same encrypting/decrypting effect)?

Deduct 36 to the positive number and you get the equivalent key. Example if k=4 then we would receive the same result if we used k = 4-36 = -32

3. Compute Ecc(M, K) for M = “COMP189” with K = 1 4 3

143 % 36 = 35 ➔ K=143 == 35

Ecc("COMP189", 143) = Ecc("COMP189", 35) = BNLO078

4. What are the total number of length 3 keys (assuming a Caesar cypher)?

There are 36^3 = 46,656 possible keys of length 3

4. Encryption (12 pts)

Complete the following exercise using an ASCII-to-binary translator.
Below, show all your work - in particular, show all the binary sequences you generate and use along the way.

1. Convert your first name into ASCII-formatted binary (1 byte per letter). Write the binary sequence out, grouping bits into groups of 4, as was done with the word "HELLO" in the lecture.

"Parsa"
P: 0101 0000
a: 0110 0001
r: 0111 0010
s: 0111 0011
a: 011 00001

Grouping them together: 0101 0000 0110 0001 0111 0010 0111 0011 0110 0001

2. Generate a random 6-bit binary key.

110100

3. Encrypt your name using the XOR function.

M: (Parsa)
0101 0000 0110 0001 0111 0010 0111 0011 0110 0001
K: (110100)
1101 0011 0100 1101 0011 0100 1101 0011 0100 1101

X:
1000 0011 0010 1100 0100 0110 1010 0000 0010 1100

4. Now decrypt your name using the XOR function as was shown in class.

X:
1000 0011 0010 1100 0100 0110 1010 0000 0010 1100
K:
1101 0011 0100 1101 0011 0100 1101 0011 0100 1101

M:
0101 0000 0110 0001 0111 0010 0111 0011 0110 0001

Discussion

In the following questions, give an answer using no more than 4 sentences.

1. Password Protection (6 pts)

You forget your password for Minerva and upon clicking “I forgot my password”, Minerva offers to email you your current password. What troubling detail does this reveal about the security on Minerva? What is the better approach?

The issue is they do not hash the passwords, they instead save them without encrypting them. Like mentioned in question 1, if a hacker were to hack the database holding all the passwords, they would easily be able to log into all the accounts. Whereas if they did hash the passwords, they would not be able to use those accounts.

A better approach to reset the password would be to send an email which would redirect the user to a new link where you can create a new password.