MID TERM EXAM (TOTAL OF 80 POINTS)
Deadline: Thursday, October 15, 2020

Instructions:

- Do your mid sem questions individually.
- Make one PDF format file for writing your analysis/results in the format <RollNo>_mid.pdf
- Submit the Python source file in the format <RollNo>.py
- Do not zip your submissions.
- If the solution requires you to use paper, paste a good quality image of the solution in the document that you are submitting.
- Queries, if any can be posted on google classroom.
- Note: Answer the questions in bullet points. Keep your responses crisp and to the point.

---

1. Assume that passwords have length 6 and all alphanumeric characters, upper and lower case can be used for the construction. How long will a brute force attack take on average if:
   a. It takes one tenth of a second to check a password?
   b. It takes a microsecond to check a password?
   c. Repeat the same for a password of length 7 and comment on the time difference you observed.
   d. If you are given 80% of the password, how does a change in length affect time taken to crack the complete password? Did the new information make your task easier? why / why not?

[3 + 1 + 1 + 2]= [7 marks]

2. Estimating the cost to recover from an attack, drives organizations to proactively invest in security.
   a. Is there a way to estimate the cost of victimization of identity theft / fraud? What will be your method to estimate the same?
   b. What is the difference between identity theft and identity fraud?

[2 + 2]= [4 marks]

3. Passwords are entered by users and checked by computers. We have been assuming that the communication channel carrying passwords from user to computer is secure. From the fingertips of the user to the authentication message from a computer, list down atleast 4 techniques you studied to secure the process. Draw a flowchart with security measures at each step of the process.

[4 +2]=[6 marks]

4. What is the difference between Groups and Roles in Access Control Schemes?

[2 marks]

5. Answer the following questions:
    a. Are there any differences between PII perception in CCPA [California Consumer Privacy Act] and GDPR, what do the differences mean?
    b. Why is “Customer loyalty history” private information?
    c. Did you know that providing a mobile number at Big Bazaar billing counter is optional? Give a reason why any vendor can not enforce you to provide a mobile number?
    d. Why did the use of the “Food Monk” app in the canteen lead to a backlash among students? Give a scenario where Food Monk can use data aggregation alongside PII to provide intelligence to Swiggy?

[3 + 3 + 3 + 3]=[12 marks]

6. Stuxnet was a targeted malware attack. Consider a novel virus like SARS-CoV-2, but in the digital space. Just like covid this computer virus spreads by contact. Draw parallels between human movement and information flow over the internet, and comment on the possibility of a digital pandemic.

[3 marks]

7. In their Differential privacy overview Apple Co. states “Apple retains the collected data for a maximum of three months”. Given that the data is already used in these three months to train ML models, how does limited retention of data mean better privacy?

[3 marks]

8. Answer the following questions:
    a. Refer to Google’s data deletion policy. What are the advantages of logical deletion over cryptographic erasure?
    b. Enumerate at least 6 different types of data erasure methods, and describe in one liner.

[3 + 6]=[9 marks]

9. You have collected a million profiles of users on a social network. Now you plan to publish this data publicly owing to the value it holds for the research community. What steps will you take before making the data public? What terms and conditions would you put for fair use?

[2 + 2]=[4 marks]

10. Look up “timing attack” in network security context. What are the current strategies followed in TOR networks to counter a timing attack. How effective is the timing attack in protocol characterization of non-TOR networks?

[3 marks]

11. Answer the following questions:
    a. Write a python program for shift cipher, where the key is ‘n’.
    Input: message, n - [m is a string, n is a number given in separate lines]
    Output: ciphertext - [print just the string output]
    b. When an involuntary key K is used, the same function F can be used for encryption and decryption. Find all involutory keys in “shift cipher” if 26 alphabets are considered for communication [a-z].

[5 + 3]=[8 marks]

12. A “fixed plain text” X when passed through an encryption function F gives a ciphertext C, which is same as plain text X . Do fixed plain texts exist in RSA encryption schemes? Prove your answer by an example.

[5 marks]

13. Answer the following questions:
    a. How is l-diversity achieved using k-anonymization? Explain with an example?
    b. How to ensure that the data does not lose the distribution while choosing which column to use for anonymization.

[3 + 2]=[5 marks]

14. How does shoulder surfing & keylogger act as a catalyst to social engineering attacks?

[2 + 2]=[4 marks]

15. Take (length of your first name) mod 2.

    If the answer is 0: make the data in table below “2-anonymised”
    If the answer is 1: make the data in table below “3-anonymised”

    Submit the anonymised table.

Customer ID	Name	Place	City	Country	No items purchased	Price
'C00013'	'Holmes'	'London'	'London'	'UK'	'2'	'6000.00'
'C00001'	'Micheal'	'New York'	'New York'	'USA'	'2'	'3000.00'

'C00020'	'Albert'	'New York'	'New York'	'USA'	'3'	'5000.00'
'C00025'	'Ravindran'	'Bangalore'	'Bangalore'	'India'	'2'	'5000.00'
'C00006'	'Shilton'	'Torento'	'Torento'	'Canada'	'1'	'10000.00'
'C00002'	'Bolt'	'New York'	'New York'	'USA'	'3'	'5000.00'
'C00018'	'Fleming'	'Brisban'	'Brisban'	'Australia'	'2'	'7000.00'
'C00021'	'Jacks'	'Brisban'	'Brisban'	'Australia'	'1'	'7000.00'
'C00019'	'Yearannaidu'	'Chennai'	'Chennai'	'India'	'1'	'8000.00'
'C00005'	'Sasikant'	'Mumbai'	'Mumbai'	'India'	'1'	'7000.00'
'C00007'	'Ramanathan'	'Chennai'	'Chennai'	'India'	'1'	'7000.00'
'C00022'	'Rushi'	'Mumbai'	'Mumbai'	'India'	'2'	'7000.00'

[5 marks]