CSE 345/545: Foundations to Computer Security
MID-SEMESTER EXAM (TOTAL OF 100 POINTS)
Deadline: 24 hrs

Instructions:

- Do your questions individually.
- Make one PDF file for writing your solutions in the format <RollNo>_MIDSEM.pdf
- State your assumptions (if any) in your solutions.
- All the queries must be posted in the classroom. No response will be provided for unreasonable queries.
- **Note: Answer the questions in bullet points. Keep your responses crisp and to the point.**

---

1. [Privacy]

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

      If the answer is 0: make the data in the table below "2-anonymised"

      If the answer is 1: make the data in the table below "3-anonymised"

   Submit the anonymized table. **[5]**

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'	'Toronto'	'Toronto'	'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'

b. The Social Science Department of IIIT-Delhi is conducting a survey where they ask participants whether they smoke or not. They want to do their best in protecting the privacy of the participants and they need your help. Prepare dummy data of participant's email addresses, and whether they smoke or not. Choose any of the techniques you have learned during the class to protect the privacy of the participants. Explain why you chose it, along with its application on the dummy data you created. **[5]**

2. [Compliance]

   Suppose you are asked to build an e-commerce platform like Amazon. A basic building block of such a platform is a payment gateway. It is absolutely necessary to follow the standard practices put in place by the governing authorities on the application dealing with underlying data. Mention these practices as per your understanding. Try to keep your answer in bullet points. Hint: What is the common term used for companies that deal with online transactional information. **[10]**

3. [Cryptography]

   Consider the following cryptography library's API:

[**5 * 6 = 30**]

Variable name	**Meaning**
m	Message in plain text
private_alice	Alice's private key. Only available with Alice.
public_alice	Alice's public key. Everyone knows Alice's public key.
private_bob	Bob's private key. Only available with Bob.
public_bob	Bob's public key. Everyone knows Bob's public key.
sym	A symmetric key
encrypt(m, k)	A function that encrypts 'm' using the key 'k' and returns a ciphertext 'c'. Ex: DSA, AES

concat(a, b)	Concatenates a and b. *Assume* that the receiving party has access to a function that splits a concatenated message perfectly, hence they know how to unambiguously identify a and b.
hash(m)	A generic hash function that takes ‘m’ as input and gives the hash ‘h’ as output. Ex: SHA-256 A hash is used to verify if the received message is the same as the one sent to them.
sign(m, k)	A signature function that takes message ‘m’ and key ‘k’ and returns a signed message ‘m’. Signatures are signed by private keys, and a public key is used to verify the signature.

Alice is sending the following messages to Bob in the specified order.

a. encrypt(concat(m, hash(m)), public_alice)
b. encrypt(concat(m, hash(m)), public_bob)
c. encrypt(m, public_bob)
   sign(hash(m), private_alice)
d. encrypt(m, public_bob) ; sign(hash(m), private_bob)
e. encrypt(sym, public_alice) ; encrypt(sym, public_bob) ; encrypt(m,sym)
f. encrypt(sym_1, public_alice)
   encrypt(sym_1, public_bob)
   encrypt(sym_2, public_alice)
   encrypt(sym_2, public_bob)
   encrypt(encrypt(m, sym_2), sym_1)
   sign(sym_1, private_alice)
   sign(sym_2, private_alice)

For each of these, answer the following:

Is it possible for Bob to decrypt the message?

If Bob can successfully decrypt a message, comment about 1) confidentiality 2) non-repudiation 3) steps to decrypt the message.

4. [Components of Security]

   The Professor has planned yet another heist. The plan is to steal all the submissions that your classmates have done so far for the FCS course. The TAs and the instructor have access to the submissions, and might or might not have a local copy of them in their systems. The Professor has asked you to prepare an assessment report for the heist. Prepare the required report. Try to keep your answer in bullets points. **[10]**

5. [Introduction to Computer Security]
   a. An ideal password authentication scheme has to withstand a number of attacks. Describe five of these attacks. **[5]**
   b. Describe the goals an ideal password authentication scheme should achieve. **[5]**
   c. A system allows the user to choose a password with a length of one to eight characters, inclusive. Assume that 10,000 passwords can be tested per second. The system administrators want to expire passwords once they have a probability of 0.10 of having been guessed. Determine the expected time to meet this probability under each of the following conditions. **[3]**
      i. Password characters may be any ASCII characters from 1 to 127, inclusive.
      ii. Password characters may be any alphanumeric characters ("A" through "Z," "a" through "z," and "0" through "9").
      iii. Password characters must be digits.
   d. A computer system uses biometrics to authenticate users. Discuss ways in which an attacker might try to spoof the system under each of the following conditions.
      i. The biometric hardware is directly connected to the system, and the authentication software is loaded onto the system.
      ii. The biometric hardware is on a stand-alone computer connected to the system, and the authentication software on the stand-alone computer sends a "yes" or "no" to the system indicating whether or not the user has been authenticated. **[2]**

6. [Access Control]
   a. Explain how access control lists are used to represent access control matrices. Describe the environments in which they are widely used and their advantages and disadvantages. **[6]**
   b. Given the security levels TOP SECRET, SECRET, CONFIDENTIAL, and UNCLASSIFIED (ordered from highest to lowest), and the categories A, B, and

C, specify what type of access (read, write, both, or neither) is allowed in each of the following situations. Assume that discretionary access controls allow anyone access unless otherwise specified.

i. Paul, cleared for (TOP SECRET, { A, C }), wants to access a document classified (SECRET, { B, C }).
ii. Anna, cleared for (CONFIDENTIAL, { C }), wants to access a document classified (CONFIDENTIAL, { B }).
iii. Jesse, cleared for (SECRET, { C }), wants to access a document classified (CONFIDENTIAL, { C }).
iv. Sammi, cleared for (TOP SECRET, { A, C }), wants to access a document classified (CONFIDENTIAL, { A }).
v. Robin, who has no clearances (and so works at the UNCLASSIFIED level), wants to access a document classified (CONFIDENTIAL, { B }). **[5]**

c. Suppose the following groups are defined for a system's access control lists:

– Group1: Alice, Bob, Cynthia, David, Eve

– Group2: Alice, Bob, Cynthia

Suppose the access control list for File 1 is:

– File 1: Group 1, R; Group 2, RW

If Alice wants to write to File 1, state whether Alice will be allowed to do so if:

i) first relevant entry policy is applied

ii) any permission in list policy is applied

Also, explain the reason for your answer. **[2+2]**

7. [Network Security]

a. A network consists of n hosts. Assuming that cryptographic keys are distributed on a per-host-pair basis, compute how many different keys are required. **[1]**
b. An X.509 certificate revocation list contains a field specifying when the next such list is expected to be issued. Why is that field present? **[1]**
c. Can we always trust a Certificate Authority (CA)? Why or why not? **[2]**
d. Turn on your phone's hotspot and connect your laptop to the network. Check your IP address. Is it Ipv4 or Ipv6? Share a screenshot of the IP address as well. Also, state the advantages and disadvantages of the type of IP address you get. **[1+2+2]**

8. How many classes did you attend so far? **[1]**