Student name: _____ Student ID: _____

CSE 345/545 Foundations to Computer Security

Mid-Sem Exam

Deadline: 2359hrs, September 29 2023

Instructions:

- Take home. Open book/notes. Individual Assignment. Discussion among peers is not allowed.
- Provide brief and specific solutions (in terms justification for techniques, tools, capabilities). More the details, higher the points.
- Make necessary assumptions.
- Handwritten solutions will not be accepted.

Time allowed: 24hrs. Total: 90 [+10 Bonus] points

1. Privacy [20]

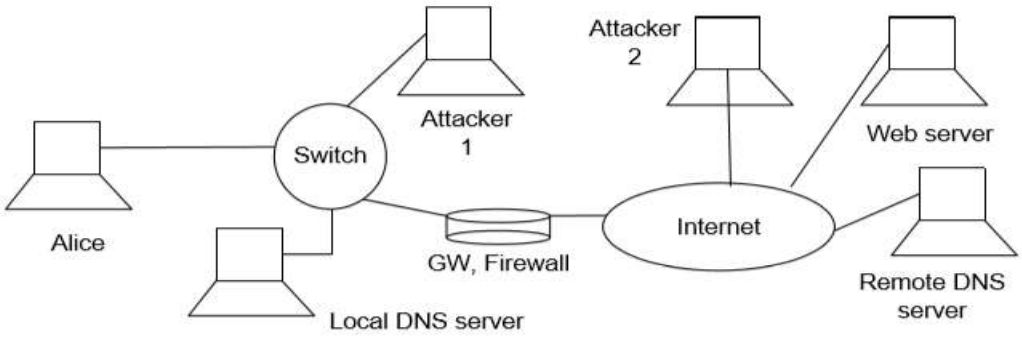
a. Apply K-Anonymity with value of K as 2 and 3. Submit the anonymized tables. [6]

Name	Age	Gender	Height	Weight	State of domicile	Religion	Disease
Ramsha	30	Female	165cm	72kg	Tamil Nadu	Hindu	Cancer
Yadu	24	Female	162cm	70kg	Kerala	Hindu	Viral infection
Salima	28	Female	170cm	68kg	Tamil Nadu	Muslim	Tuberculosis
Sunny	27	Male	170cm	75kg	Karnataka	Parsi	No illness
Joan	24	Female	165cm	71kg	Kerala	Christian	Heart-related
Bahuksana	23	Male	160cm	69kg	Karnataka	Buddhist	Tuberculosis
Rambha	19	Male	167cm	85kg	Kerala	Hindu	Cancer
Kishor	29	Male	180cm	81kg	Karnataka	Hindu	Heart-related
Johnson	17	Male	175cm	79kg	Kerala	Christian	Heart-related
John	19	Male	169cm	82kg	Kerala	Christian	Viral infection

b. What techniques (at least two) would you do to increase the utility of the above anonymized data? Demonstrate. [7]

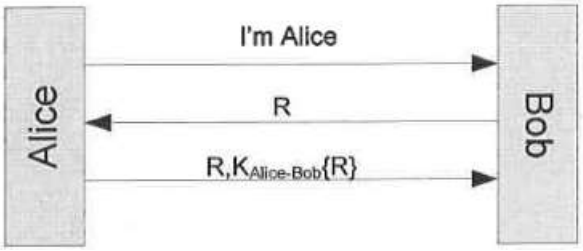
c. Academic department of IIIT-Delhi wants to conduct a survey for outgoing students about their experience. They want to do their best in protecting the privacy of participants' and they need your help. Prepare dummy data of participants. Choose techniques you have learned during the class to protect the participant's privacy in line with GDPR requirements. Explain why you chose it, along with its application on the dummy data you created. [7]

2. ***Network Security [25+5]***



(a) Describe how attacker 1 to perform DNS poisoning attack. Describe step-by-step procedure. [6]
(b) Attackers can DDoS your website. How would you efficiently mitigate the attack and restore access to your site from both the attackers? Defend your solutions [8]
(c) How would you set up a secure communication channel for each device in the above architecture? [Bonus if you can set it up without involving third-party service and offline key exchange?] [5+5].
(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+3]

3. Authentication [20]



(a) Suppose we are using a three-message mutual authentication protocol and Alice initiates contact with Bob. Suppose we wish Bob to be a stateless server, and therefore it is inconvenient to require him to remember the challenge he sent to Alice. Alice sends the challenge back to Bob, along with the encrypted challenge. Is the protocol (presented below) secure? Justify your answer. [4]
(b) Is a common key necessary for setting up secure communication channel? How can both parties' safely setup a common key? What are its limitations? [6]
(c) How can the above limitations be overcome to set up secure communication channel, is it possible for attacker(s) to launch successful MITM or spoofing attacks? Justify [6].
(d) Can you perform mutual authentication if only one party has verifiable certificate, if yes what cryptographic information do we use set up secure comm? Is it secure? Why? [4]

4. Access Control [10]

Consider the following scenario. Alice owns file Z. Alice has read and write access to file X and write access to file Y. Bob owns file X. Bob has read access to file Y and read, write, and execute access to file Z. Carol owns file Y. Carol has read access to files X, Y, and Z.

a. Given a system with many transient users and several persistent protected resources, which technique, ACL or Capabilities, is more efficient for storing and managing users' permissions? Give justifications for your answer. [2]
b. In ACL/Capability is it possible for an unauthorized user/process to misuse privileges of Alice to write/read contents of file X? How? [4]
c. How can you prevent such unauthorized access? Elaborate your response. [4]

5. Network Anonymity [15+5]

a. Is perfect anonymity possible on Internet? Provide justification for either of your answers. [4]

b. How does tools such as TOR build secure anonymous communication channel with acceptable QoS? Explain. [6]

c. Can anonymity in TOR be compromised? Justify. How would you exploit vulnerabilities (at least 2)? [Bonus if you provide zero-day exploits] [5+5]