Student name: ___________________________________ Student ID: ______________________

CSE 345/545 Foundations to Computer Security

Mid-Sem Exam

Due: 2359hrs, March 2 2025

Plagiarism policies will be strictly enforced

Total Points: 85+15

Instructions:

- Take home. Open Book (Internet Access Allowed). Discussion among peers is not allowed.
- Use of GPT-based tools are not allowed
- Provide brief and specific solutions (in terms justification for techniques, tools, capabilities). More the details, higher the points.
- Make necessary assumptions. Justify all your answers.

1. ***Privacy [25]***

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

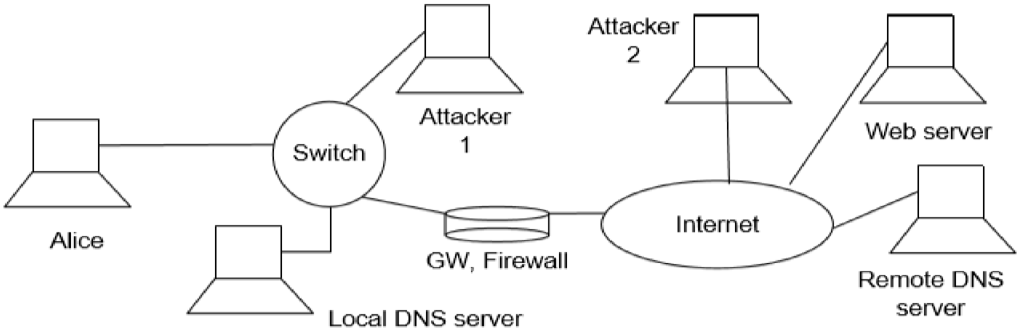
Pin Code	Age	Gender	Acc Balance
110020	33	M	150000
110045	31	M	250000
110045	39	M	200000
110020	38	M	250000
113420	69	F	850000
113420	67	F	150000
113421	55	F	850000
113421	50	F	200000
110045	45	M	280000
110045	46	M	450000
110020	47	M	850000
110020	41	M	450000

B. What techniques (at least two) would you do to increase the utility of the above anonymized data? Demonstrate. [5]

C. Academic department of IIIT-D wants to conduct a survey of outgoing students about their experience, which could be potentially be sent to third-party for analysis. They want to do their best in protecting the privacy of participants' and they need your help. 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 data (you may create dummy data if needed). [7]

D. What sort of guarantees does the technique described in (c) provide for privacy preservation? Explain with mathematical proof/theorems. Also, describe specific scenarios where they fail [7]

2. ***Cyber Attacks [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]

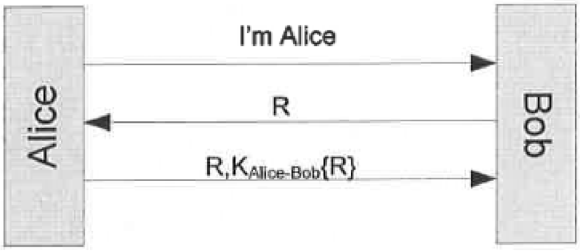
3. ***Building Secure Communication [10]***

In building your group project.

(a) How would you compromise the HTTPS connection. Describe in detail

(b) Provide a reasonable solution to counter such an attack? Describe its feasibility and effectiveness.

4. ***Authentication [10+10]***



(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 above) secure? Justify your answer. [5]

(b) 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? [5]

Bonus [10]: Provide a usable decentralized system with Blockchain for issuing certificates as an alternative for centralized CAs. Propose a Protocol. Explain its feasibility.

5. ***Network Anonymity [15]***

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

(b) What are the principles and technique that tools like TOR rely on to provide anonymity for users? Justify. [5]

(c) What are the potential vulnerabilities in TOR that you, as a malicious third party, can exploit to degrade the anonymity of users? Justify. How would you go about exploiting them? [6]