Strathmore UNIVERSITY

SCHOOL OF COMPUTING AND ENGINEERING SCIENCES
BACHELOR OF SCIENCE IN INFORMATICS AND COMPUTER SCIENCE
CNS 4204: PRIVACY ENHANCING TECHNOLOGIES
END OF SEMESTER EXAM

Date: 4th December 2024 **Time:** 08:00-10:00 Hours

Instructions:
This Examination consists of **FIVE** questions
Answer **Question ONE (COMPULSORY)** and any other **TWO** questions.

QUESTION ONE (30 MARKS)

a) Privacy Concerns and Data Protection: Maisha.org a non-Governmental organization collects vast amounts of user data through its mobile application. While the company claims to anonymize and aggregate this data for research purposes, reports surface suggesting that individual user identities can be de-anonymized with relatively simple techniques. Furthermore, there are allegations of data breaches and unauthorized access to sensitive user information.

Required

i. Using advanced cryptographic techniques, propose a secure method for data anonymization that maintains usability for research while ensuring user privacy. (4 marks)

ii. Evaluate two potential vulnerabilities and discuss strategies to mitigate them. (2 marks)

b) Identify and explain two anonymous properties (2 marks)

c) Describe two families of privacy technologies, and clearly distinguish them based on their assumptions and threat models? (4 marks)

d) How can PETs help with data protection compliance? (3 marks)

e) PETs can effectively reduce risk to people. However, the resulting information may be less useful compared with the original information. This is because using these techniques can reduce how close the randomized answers to queries are compared to the real ones (ie those without "noise" applied).

Required

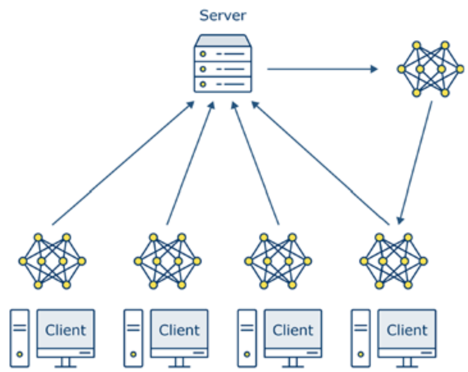
With a suitable example, analyze two PETs that derive or generate information that reduces or removes people's identifiability (5 marks)

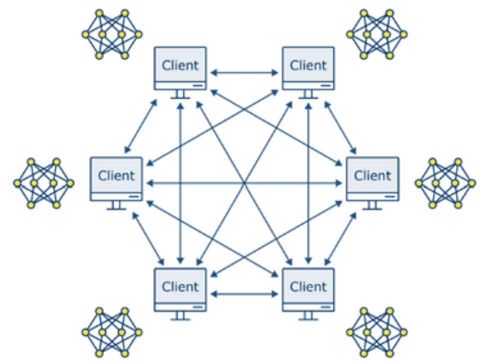
f)

i. What is homomorphic encryption and what does it do? (3 marks)

ii. How does HE assist with data protection compliance? (3 marks)

g) Federated learning (FL) is a technique that allows multiple different parties to train AI models on their own information ('local' models). Study the two approaches below and answer the following questions?





Required

a) Identify each approach above and describe its operation? (4 marks)

<u>QUESTION TWO (15 MARKS)</u>

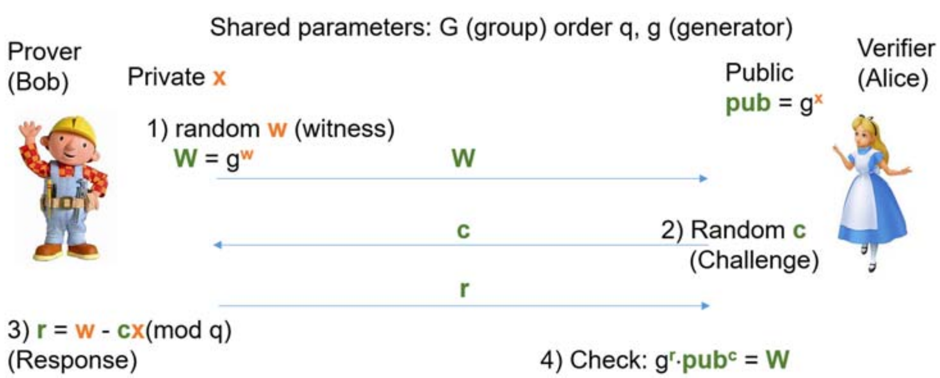
a) The requirement of harm has significantly impended the enforcement of privacy law. In most tort and contract cases, plaintiffs must establish that they have suffered harm. Sketch an Illustrated taxonomy of Privacy Harms (8 marks)

b) Analyse two risks of using PETs? (4 marks)

c) What is cool about homomorphic schemes? (3 marks)

<u>QUESTION THREE (15 MARKS)</u>

Examine the Schnorr Identification Protocol for Zero-Knowledge, and answer the following questions?



Required

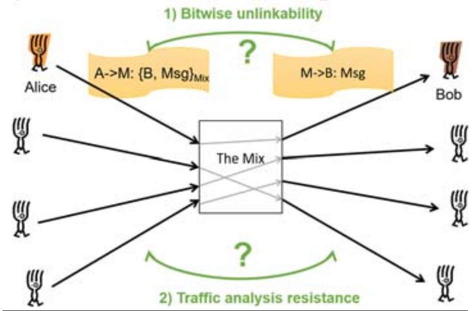
i. Does the verification work? (5 marks)

ii. Does that prove Bob knows x? (5 marks)

iii. Are we leaking any information about x? (5 marks)

<u>QUESTION FOUR (15 MARKS)</u>

a) Below illustration depicts the mix – security issues



Required

i. Describe two general designs for anonymous communication? (4 marks)
ii. Briefly distinguish the mix security issues in the illustration above. (4 marks)

b) Bob is running a hidden service on top of Tor and wants to know how frequently he should choose new introduction points. Bob cares about his identity not being exposed, and about the availability of his service. Help Bob make an informed choice by explaining the costs and benefits of rotating introduction points either more or less frequently. (7 marks)

<u>QUESTION FIVE (15 MARKS)</u>

a) In Cryptography, properties of a system - define two requirements for public-key encryption schemes: (6 marks)
b) Considering additively homomorphic public-key encryption, also as discussed by Benaloh Crypto-system. describe four essential algorithms of a proper FHE scheme. (9 marks)