Strathmore
UNIVERSITY

SCHOOL OF COMPUTING AND ENGINEERING SCIENCES
BACHELOR OF SCIENCE IN COMPUTER NETWORKS AND CYBER SECURITY
CNS 4204: PRIVACY ENHANCING TECHNOLOGIES
END OF SEMESTER EXAMINATION

DATE: 6th December 2023 **Time: 15:30-17:30 Hours**

Instructions

1. This examination consists of **FIVE** questions.
2. Answer **Question ONE (COMPULSORY)** and any other **TWO** questions.

Question 1: General Questions (30 marks)

1. Define homomorphic encryption and provide an example of a real-world application where it can be used for secure data analysis (6 marks).

2. Explain the concept of "k-anonymity" in the context of privacy preservation. How does it enhance privacy in data analysis? (6 marks).

3. Discuss the main principles of Privacy by Design and provide an example of a real-world application where it has been successfully implemented (6 marks).

4. What are the key challenges associated with implementing anonymous channels, and how can they be mitigated? (6 marks).

5. In the context of e-Passports and e-Payment, explain the importance of cryptography and privacy implementation techniques. Provide an example of a situation where these techniques are crucial (6 marks).

Question 2: (15 marks)

1. i) In the context of location privacy, explain what geofencing is and how it can be used to enhance privacy (5 marks).

   ii) Provide a practical example where geofencing can be applied. (2 marks)

2. Discuss the challenges in preserving privacy in distributed systems and the techniques used to address these challenges (8 marks).

Question 3: (15 marks)

1. Explain the concept of multi-factor authentication (MFA) and its role in enhancing security and privacy, providing real life situations where MFA is crucial (7 marks).

2. Discuss the importance of attribute-based access control (ABAC) in authorization and privacy. How does it differ from role-based access control (RBAC)? (8 marks).

Question 4: (15 marks)

1. Define Zero Knowledge Proofs (ZKPs) and explain their significance in privacy preservation. Provide an example of an application of ZKPs in the real world (8 marks).

2. In the context of genomic data privacy, discuss the risks associated with data breaches and the regulatory frameworks that address these risks (7 marks).

Question 5: (15 marks)

1. Explain how the M-Pesa mobile money system in Kenya relies on cryptography to secure transactions and user data. (7 marks)

2. Explore how the Kenyan government implemented differential privacy to conduct a census that respects citizens' privacy. (8 marks).