Departament of Informatics Engineering

Security and Privacy, MECD

Name: **Student number:**

1. Computer security concepts

1.1. From the following tools/mechanisms, select those that can be used for confidentiality.

A) Digital signatures B) access control

C) checksums D) digital signatures

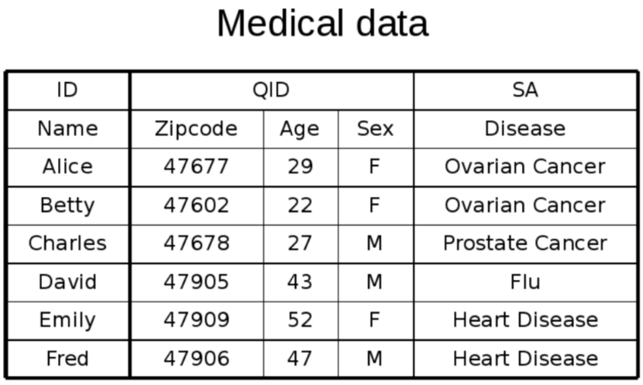
1.2. The integration of multiple data sources and information flows to determine the source of a particular data stream or piece of information is called _____________.

A) authentication B) access control

C) authorization D) de-identification

2. Privacy-preserving Data Publishing

2.1. Based on the example dataset below, explain the concept of equivalent class, providing an example resorting to one of the basic anonymization operations



Medical data

ID	QID			SA
Name	Zipcode	Age	Sex	Disease
Alice	47677	29	F	Ovarian Cancer
Betty	47602	22	F	Ovarian Cancer
Charles	47678	27	M	Prostate Cancer
David	47905	43	M	Flu
Emily	47909	52	F	Heart Disease
Fred	47906	47	M	Heart Disease

2.2. Explain the drawback of k-anonymity, and how l-diversity aims to address it.

2.3. Calculate the distinction and separation of the following example dataset for the attribute **sex**.

	age	sex	state
1	20	Female	CA
2	30	Female	CA
3	40	Female	TX
4	20	Male	NY
5	40	Male	CA

3. Secure Multiparty Computation (SMC) and Privacy

3.1. In SMC two or more parties wish to jointly compute a function of their inputs while preserving certain security properties, such as privacy, correctness and independence of inputs. Considering the auction example, where users bid for a product, explain what privacy **and** correctness mean in this context.

3.2. In oblivious transfer, the receiver chooses one key-pair (pk1, sk1) and one public-key pk2 without corresponding private-key, thus sending pk1 and pk2 to the sender. The sender has 2 messages m0 and m1, and wants the receiver to get access to m0 without knowing m1 or vice-versa. For that, the sender encrypts m0 with pk1 and m1 with pk2, resulting respectively in c0 and c1. It then sends c0 and c1 to the receiver.

This protocol assumes that the receiver is semi-honest. Explain why the receiver has to be semi-honest and how can a receiver that is not semi-honest compromise the system and have access to both messages?

4. Cryptography

4.1. Explain RSA Encryption and Decryption with an example.

5. Homomorphic Encryption

5.1. How Integer-Based Secret Key Scheme work?

6. 6. Adversarial machine learning

6.1. What are typical attacks to machine learning algorithms? Explain with examples.

7. 7. Searchable Encryption

7.1. Explain, with an example, how index-based searchable encryption work.