1 2 9 0 Departamento de Engenharia Informática
FACULDADE DE CIÊNCIAS E TECNOLOGIA
UNIVERSIDADE D COIMBRA

Security and Privacy – MECD
Exame Normal - 17 de Janeiro de 2022
90 minutos (*sem consulta*)

Nome: **Nº Aluno:**

1. (1.5 v) Explain one key security and/or privacy challenge that affects particularly data scientists.

2. (1.5 v) Padding is necessary in most encryption scenarios even if for diverse purposes. What is the particular importance of padding together with RSA?

3. (1.5 v) Explain why you should not rely on RSA to exchange/agree on keys and what is the main advantage of using an algorithm such as Diffie-Hellman.

4. (1.5 v) Discuss what would make homomorphic encryption so useful for data scientists and why it is not still applicable in the current forms.

5. Considering the presented dataset, answer to the following:

	age	**sex**	**district**	**disease**
1	30	Male	Coimbra	cancer
2	20	Male	Lisboa	rhinitis
3	40	Male	Porto	cancer
4	39	Male	Braga	Covid-19
5	20	Male	Lisboa	rhinitis
6	30	Male	Coimbra	rhinitis
7	40	Male	Porto	e.disfunction
8	20	Male	Lisboa	cancer
9	30	Male	Coimbra	rhinitis
10	39	Male	Braga	Covid-19

a) (1.0 v) identify the most suitable quasi-identifier, justifying

b) (1.5 v) determine the **k** for your answer to a)

c) (3.0 v) propose concrete operations to increase the **k**, indicating the resulting dataset and the respective **k**.

1				
2				
3				
4				
5				
6				
7				
8				
9				
10				

Final k=

6. (1.5 v) Deterministic encryption can be used to achieve searchable encryption. Indicate an algorithm that could be used to implement this strategy and indicate the problems of adopting such strategy.

7. (2.0 v) Present three principles of privacy protection (which are based in the fair information practices). Explain briefly each one of them.

8. (2.0 v) In our practical assignment you used more than one privacy model. Indicate one of the privacy models that you used, together with its advantages and limitations.

9. (2.0 v) Classify the following sentences as true or false, justifying the ones classified as true and correcting the ones classified as false.

a. Performance is not relevant when considering techniques to protect data security.
b. Removing personally identifiable information solves all privacy issues.
c. Differential privacy is not secure for sequential composition.
d. The amount of noise to add in differential privacy is only influenced by the level of protection desired.

10. (1.0 v) Assume that you are developing an application that processes data and that this application can be configurable by the user through input data such as numeric values, dates and arbitrary text. Explain only one vulnerability type that you should be concerned with, and how you can avoid it.