1 2 9 0

Departamento de Engenharia Informática
FACULDADE DE CIÊNCIAS E TECNOLOGIA
UNIVERSIDADE D COIMBRA

Security and Privacy – MECD
Exame Normal - 11 de Janeiro de 2020
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. (1.0 v) Deterministic encryption can be used to achieve searchable encryption. Indicate the problem of adopting such strategy.

6. (2.0 v) Present three principles of privacy protection (which are bases in the fair information practices). Explain briefly each one of them.

7. (1.0 v) From the following tools/mechanisms, select those that can be used for confidentiality.

A) Encryption B) Digital signatures C) pseudonyms D) data correcting codes

8. (1.5 v) Calculate the distinction and separation of the following dataset, considering the pair of attributes {age, state}. Explain your answer.

	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

Nome: **Nº Aluno:**

9. (1.5 v) One can identify 4 basic anonymization operations: generalization, suppression, anatomization and perturbation. Explain how to use generalization.

10. (2.0 v) Explain the limitations of k-anonymity that l-diversity tries to address, and how it tries to do so.

11. (2.0 v) 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 product, explain the key properties to be preserved.

12. (1.0 v) Explain briefly what you understand by adversarial machine learning.

13. (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 / explicit identifiers is and effective measure for anonymity protection.
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.