

Cryptography programming exercise

Code: https://github.com/gicanon/simple_caeser_encryption

- Why did you select the algorithm you chose?
- Would it meet the GDPR regulations? Justify your answer.

I chose the ceaser cryptography algorithm because it is one of the most straightforward and widely known encryption techniques (TutorialPoint, 2020). Each letter of the plaintext is replaced by a letter in a certain number of places in the alphabet.

Furthermore, as a beginner in this section, starting with the simplest one is always great for understanding its logic.

Unfortunately, the Ceaser Cipher algorithm is not secure overall. There is a limitation to the possible number of passwords. The password is just a shift, and patterns are recognizable especially double numbers. Furthermore, Brute Force Technique is also a method for trying every possible decryption key. It take less work and it is very simple to use for a hacker (TutorialPoint, 2020).

References

TutorialPoint, 2020. Cryptography with Python - Quick Guide.

Available from:

https://www.tutorialspoint.com/cryptography_with_python/cryptography_with_python_quick_guide.htm [Accessed 9 November 2022].