Unit 8: Seminar Preparation

Title: Cryptography Programming Exercise

Question:

Read the Cryptography with Python blog at tutorialspoint.com (link is in the reading list). Select one of the methods described/ examples given and create a python program that can take a short piece of text and encrypt it.

Create a python program (you can use the Jupyter Notebooks space) that can take a text file and output an encrypted version as a file in your folder on the system. Demonstrate your program operation in this week's seminar session.

Answer the following questions in your e-portfolio:

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

We will review your work from Unit 7 (Python Shell) in this week's seminar, as well as this cryptography activity. There will also be an opportunity to review your team's assignment progress during the seminar.

Remember to record your results, ideas and team discussions in your e-portfolio and complete the activities in Unit 7.

Response:

Why did you select the algorithm you chose?

I selected the Fernet symmetric encryption method for this project due to its strong security features and ease of implementation. Fernet ensures the confidentiality and integrity of the data by providing

encryption and decryption processes that are both simple and effective (Pronika & Tyaki, 2021). The algorithm uses AES encryption in CBC mode, along with a SHA256 hash to ensure data authenticity (Pronika & Tyaki, 2021). This combination offers a robust level of security, making it suitable for protecting sensitive information. Additionally, the library used to implement Fernet is well-documented and widely adopted in the Python community, which further supports its reliability for practical applications.

Would it meet the GDPR regulations? Justify your answer.

Yes, using the Fernet encryption method would help in meeting GDPR regulations. The General Data Protection Regulation (GDPR) emphasizes the need for secure processing of personal data to protect individuals' privacy. By encrypting data, we can significantly reduce the risk of unauthorized access and data breaches (General Data Protection Regulation, 2018). Even if the encrypted data is intercepted, it remains unreadable without the corresponding decryption key. However, it is crucial to implement strong key management practices, as the security of the encrypted data relies heavily on the protection of the encryption key (GDPR, 2018). By ensuring that the key is stored securely and is only accessible to authorized personnel, we can further enhance compliance with GDPR requirements related to data protection and security.

References:

General Data Protection Regulation (GDPR) 2018, c. 2. Available from: https://gdprinfo.eu/ [Accessed 7 September 2024].

References:

Pronika, P., & Tyagi, S. (2021) Enhancing Security of Cloud Data through Encryption with AES and Fernet Algorithm through Convolutional-Neural-Networks (CNN). *International Journal of Computer Networks and Applications (IJCNA)* 8(4): 288-299. DOI: 10.22247/ijcna/2021/209697