Encryption Algorithms

The Reverse Cipher method of cryptography is simple in nature, and as such is simple to implement. It works by taking a string, then outputting this in reverse to deter people being able to read this easily (Tutorials Point, 2024). Below is an example of a simple block of code that carries out this function.

The Reverse Cipher was chosen for demonstration due to the visible flaws within it's construction. It's simplicity is also the major drawback with it, as the actual data doesn't change much. While it is possible that it may work for larger amounts of data, or data that isn't written using words (for example, data held in Hexi format), for simple strings such as name, addresses and email addresses it would be relatively simple to decrypt the information. Along with this, because the algorithm can be broken easily, if a mixture of simple and complex data is held, being able to decrypt the simple data makes obtaining the more complex data an easier task.

With regards to GDPR, this method of encryption would not meet the standards required for this. GDPR Article 32 mandates that data is stored in a way appropriate to the amount of risk (European Union, 2016). Given that bad actors obtain information such as names and addresses, all of which tend to be made of standard words (an address for example may end in key words such as road, street or lane), this level of encryption and it's inability to transform the data in any meaningful way would not constitute a secure storage system as per GDPR.

Reference

Tutorials Point (2024) Cryptography With Python. Available at https://www.tutorialspoint.com/cryptography_with_python/cryptography_with_python_reverse_cipher.htm [Accessed 18 October 2024]

European Union (2016). General Data Protection Regulation (GDPR). Available at: https://eur-lex.europa.eu/eli/reg/2016/679/oj [Accessed 20 October 2024]