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.

I chose the ROT13 algorithm mainly because it was easy to understand and implement. ROT stands for Rotate, and 13 refers to the character position distance for replacement, i.e., the distance between A and N is 13, therefore A is replacement with N, and so it continues along the alphabet.

The algorithm would most certainly not meet GDPR requirements, and can be easily decrypted by any party. Given how straightforward it is to break it, it violates GDPR's section (1) (5), where it is required for data to be "Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures" (ICO, 2022). Interestingly enough, it had been used to encrypt registry keys in Windows as of 2006, despite it being known for decades as unsuitable for such uses (Stevens, 2006).

References:

ICO (2022) Encryption. ICO. Available from: https://ico.org.uk/media/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/encryption-1-0.pdf [Accessed 17 December 2024]

Stevens, D. (2006) ROT13 is used in Windows? You’re joking!. Didier Stevens. Available from: https://blog.didierstevens.com/2006/07/24/rot13-is-used-in-windows-you’re-joking/ [Accessed 17 December 2024]