

'''

Read the Cryptography with Python blog at [tutorialspoint.com](https://tutorialspoint.com).  
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 that can take a text file and output an  
encrypted version as a file in your folder.  
Demonstrate your program operation in this week's seminar session.

Answer the following questions in your e-portfolio:

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

Answers:

- 1.) 3DES was chosen, which is more secure than DES used in the tutorial, because it is was simple to implement, and is a commonly available standard for symmetric key encryption (Whiteman, 2010, AWS, N.D).
- 2.) The GDPR does not specify the use of encryption in all cases, and leaves it to the discretion of the service provider with regards to the encryption algorithm used (ico, N.D). However, the GDPR does reference NIST and other international encryption standards like those specified in ISO/IEC19790 (ico, N.D). Many international standards require the use of AES, as the defacto standard (OWASP. N.D).

References:

- \* AWS. (N.D) Cryptographic Algorithms. Available from:  
<https://docs.aws.amazon.com/crypto/latest/userguide/concepts-algorithms.html>  
[Accessed 20 January 2021]
- \* ico. (N.D) Encryption. Available from:  
<https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/security/encryption/>  
[Accessed 20 January 2021]
- \* OWASP. (N.D) Cryptographic Storage Cheat Sheet. Available from:  
[https://cheatsheetseries.owasp.org/cheatsheets/Cryptographic\\_Storage\\_Cheat\\_Sheet.html](https://cheatsheetseries.owasp.org/cheatsheets/Cryptographic_Storage_Cheat_Sheet.html) [Accessed 20/12/2021].
- \* Whiteman, T. (2010) pyDES. Available from: <http://pydes.sourceforge.net/>  
[Accessed 20 January 2021]

'''

```
import pyDes
import os
```

```
plain_text = "this is a test of the 3DES cipher" #input('Please input a
sentence:\n')
key = "abcdefghijhklmnop" #input('Please input a 16 character password:\n')

encryptor = pyDes.triple_des(key, pad = ".")

cipher_text = encryptor.encrypt(plain_text)
```

```
print(cipher_text)
file = open('hidden.txt', 'wt')
for char in cipher_text:
    file.write(str(hex(char)))

file.close()
```