J. Irvine Secure Software Development

Cryptography with Python

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

Cypher Program

Code

```
letters=["a","b","c","d","e","f","g","h","i","j","k","l","m","n","o","p","q","r","s","t","u","v","w","x","y","z"]
playing = " "
final = " "
org = " "

def encrypt(str,n):
    result = []
    for x in str:
        if x == " ":
            convert = "  "
            result.append(convert)
        else:
            convert = (letters.index(x) +n) %26
            result.append(letters[convert])
    final = " ".join(result)
    print(final)
    return final

def decrypt(str,n):
    back = []
    for x in str:
        if x == " ":
            original = "  "
            back.append(original)
        else:
            original = (letters.index(x) -n) %26
            back.append(letters[original])
    org = " ".join(back)
    print(org)

str=input("\nType the word you want encrypted? ")
# This moves the letters e.g. 2 would change A to C, B to D etc.
n=int(input("\nEnter a number for the key? "))
final=encrypt(str,n)

print("\nThe text will now be decrypted. ")
# This changes the letters back to the original word.
decrypt(final,n)
```

Output

```
Type the word you want encrypted? python is a coding language

Enter a number for the key? 3
s b w k r q    l v    d    f r g l q j    o d q j x d j h

The text will now be decrypted.
p    y    t    h    o    n            i    s            a            c    o    d    i    n    g
       l    a    n    g    u    a    g    e
```

J. Irvine Secure Software Development

Answer the following questions in your e-portfolio:

- **Why did you select the algorithm you chose?**

I have chosen the Caesar Cipher algorithm. This is a simple encryption technique that moves each letter of the plaintext message by a certain number of positions down the alphabet. For example if it moved 3 places then A becomes D and B becomes E etc.

- **Would it meet the GDPR regulations? Justify your answer.**

The Caesar Cipher algorithm is not related to GDPR compliance. GDPR compliance are regulations that govern the collection, use, and storage of personal data of European Union citizens. It is not related to encryption techniques.

What is GDPR, the EU's new data protection law? - GDPR.eu