SECRET SHARING

*secret sharing schemes are schemes that split shares of a given secret among a set of trusted participants*

*: And there's two properties*

*Dynamic:* The scheme allows for a secret owner to amend the rules of a given secret securely

Secure: cryptanalytically unbreakable in its encryption model in that no holder of a share can uncover the shared secret without first gaining access to the threshold number of secret shares

Using the cryptography module in Python, we will use an implementation of AES called Fernet to encrypt data. I will also show you how to keep keys safe and how to use these methods on files

First thing I will have to install cryptography Since Python does not come with anything that can encrypt files to install this, execute

python -m pip install cryptography

For creating a key we will use

from cryptography.fernet import Fernet

() key = Fernet.generate\_key

For reading the key we will use

file = open('key.key', 'rb')

key = file.read() #The key will be type bytes

() file.close

For the Encrypting

from cryptography.fernet import Fernet

() message = "my deep dark secret".encode

f = Fernet(key)

encrypted = f.encrypt(message)

For the Decrypting

from cryptography.fernet import Fernet

encrypted = b"...encrypted bytes..."

f = Fernet(key)

decrypted = f.decrypt(encrypted)

For reading a file we will use

: with open(input\_file, 'rb') as f

() data = f.read

For calculate the run time I used

import timeit

code\_to\_test = """

a = **range**(100000)

b = []

: for i in a

b.**append**(i\*2)

elapsed\_time = timeit.**timeit**(code\_to\_test, number=100)/100

**print**(elapsed\_time)

I test the program with this plaintext: hello world, This is my secrt massage

And with this key: 8Rl\_qPwV6bX9IaQ8bXBGkQlSvzHfpYNo2pU7ms5CymY

And I got this ciphertext: gAAAAABenyU9qSKhgUymUIiWITquwvUWmx7o9Vv0abmWGhuSCCL6RGtFQ5e-JLbLyLPKPr6OrTkOB\_NpbxeMX1FWu3RUbwkA1wABYxkocTo2-eKgd0tzWE7t7w-wHvLvqiGVf-5ayytQ

And after Decrypting with the same key I get this plaintext: hello world, This is my secrt massage

After 10 runs the average it takes to generate the key = 0.017389529 sec

After 10 runs the average it takes to Encrypting the massage = 0.01930842500 sec

After 10 runs the average it takes to Decrypting the massage = 0.011889527 sec

With intel CPU Core I5 –7200U 2.5Gz boosted to 3.1Gz