COM709 FUNDAMENTALS 2020 Assignment AE1 Part 3

andy

October 1, 2020

1 Write an historic cryptography demo

1.1 Instructions

- You must follow the functional requirement specifications
- You must follow the non-functional requirement specifications
- You must deliver the product on time for the deadline
- You must deliver all parts of the product
- You must deliver the product in the specified form

1.2 Delivery date

- Thursday October 22 2020

1.3 Functional requirements

- You must write two small python programs
  - encrypt.py
  - decrypt.py
- The *encrypt.py* program is to take two iputs
  - a message from a user
  - a secret key
- It must output a ciphertext (encryted form of the message)

  - the ciphertext should also be base64 encoded
  - The *decrypt.py* program should take two inputs
    * the encrypted cyphertext
    * the secret key
  - It must output the original message as plaintext

1.4 Cipher requirements

- You may choose ANY of the following cipher methods
  - Rotation
  - Substitution
  - Modulo or XOR operations
  - Any other combination of these

1.5 Optional requirements (extra marks)

- messages, ciphertext and keys can be passed as command line arguments

1.6 Non Functional (constraints)

- Programs should be docstring commented and examinable via pydoc
- Programs to be written in Python >= v.3.20
- Programs must ONLY use specified libraries
  - buitins (os, sys, csv etc)
- Programs must execute from the command line
- Programs must be self-contained (apart from the data store)
  - two single python files

1.7 Delivery requirements

- Both programs must be named with .py extensions
- Theu should be zipped into a **.zip** archive
- the .zip file must be named as your student number
  - for example: Q1234567.zip

1.8 Marking Criteria

- Is in ZIP file with correct student number
- Folder structure is correct
- Well commented source code
- Both programs execute and return original plaintext
- Each program presents a help response if called without arguments

1.9 Example Usage Session

```
$ python3 encrypt.py
>  Please enter your message:
>  Hi Bob, we need to have a meeting
>  regarding the widget frobnication.
>  Thanks. Alice.
>
>  Please enter a secret key:
>  abracadabra
>
>  e63ef6fe36fa24937468e62b3567dc23
>  78e482ae82345fa8239cc3eaa56742645
>  63478624ce3
>
$ python3 decrypt.py
>  Please enter your ciphertext:
>  e63ef6fe36fa24937468e62b3567dc23
>  78e482ae82345fa8239cc3eaa56742645
>  63478624ce3
>  Please enter your key:
```

```
>  abracadabra
>
>  Hi Bob, we need to have a meeting
>  regarding the widget frobnication.
>  Thanks. Alice.
$
```