University of Kent

Astronomy, Space Science and Astrophysics

Cryptography Assignment

Stage 1 - PH370 Computing

Monday 19th March 2018

Report Author: Lukasz R Tomaszewski

Contents

1 Python Script

```
 1  #!/usr/bin/env python3
 2  # -*- coding: utf-8 -*-
 3  """
 4  Created on Mon Mar  5 13:01:35 2018
 5  
 6  @author: lrgtomaszewski
 7  """
 8  
 9  def getMode():
10      print('Do you wish to encrypt or decrypt a message?')
11      mode = input()
12  #This allows for the user to input the choice of encrypting a message
13  #or decrypting a message.
14      if mode in  'e encrypt'.split():
15          print(Encryption())
16          return mode
17  #If the user inputs any of the strings listed in line 14 then, it will
18  #print the encryption code. So it follows the encrytion process.
19      elif mode in 'd decrypt'.split():
20          print(Decryption())
21          return mode
22  #If the user inputs any of the strings listed in line 19 then, it will
23  #print the encryption code. So it follows the encrytion process.
24      else:
25          print('For Encryption, enter either "e", "encrypt".')
26          print('For Decryption, enter either "d", "decrypt".')
27  #If the user doesn't input any of the strings listed in line 14 & 19
28  #then, it will print the message listed in line line 25/26 so it
29  #advises the user the direct input it requires to proceed.
30  
31  def Encryption():
32      ERead = open('plaintext.txt', 'r').read()
33  #This opens the plaintext.txt file and reads it, if the user did not
34  #want to source form a txt file then the code can be replaced in line
35  #32 by;
36        #print('Enter message to be encrypted!')
37        #ERead = input()
38      print('Please enter unique key for Encryption!')
39      Ekey = input()
40  #Line 38 & 39 allows the user to input a unique key that is the
41  #important reference to which the code encrypts and decrypts, thus
42  #typing the key in has to be correct.
43      EMessage = len(ERead)
44      EKey = Ekey * (1 + EMessage//len(Ekey))
45  #Both the message and key in lines 32 & 39 are now broken down for
```

```
46 #their lengths.
47     EWrite = open('plaintext.txt.enc.txt', 'w')
48 #This is the location where the encrypted text with outputted too.
49 #This allows the code to write into a .txt file.
50     for i in range(EMessage):
51         EPi = ord(ERead[i])
52         Eki = ord(EKey[i]) - 32
53         ECi = EPi + Eki
54 #The above sequences allow for the mathematical formula for
55 #encrypting a message. Lines 51 converts the individual letters
56 #of the message into numbers that corresponds with ASCII 1967
57 #defintions. Line 52 Does the following but with the key instead
58 #of the message, 32 is then subtracted but the numbers the individual
59 #letters so that the key is not greater than 126 which is the highest
60 #number in the ASCII 1967 defintions. It is the added together to
61 #encrypt the letter via a number.
62         if ECi > 126:
63             ECi = ECi - 95
64 #If the final value of ECi is greater than 126 (The max limit of the
65 #ASCII 1967 defintions), similiar what happens to the key in line 52.
66         E = chr(ECi)
67 #Line 53 adds the key and the letter togehter to get a single number
68 #the muber is thus changed back into a letter in relation to the
69 #ASCII 1967 defintions. This allows the message in line 32 to be
70 #"encrypted" but replaces the orginal message with the encrypted
71 #message. Which is saved in a .txt file named in line 47.
72         print(EPi, Eki, ECi, E)
73         EWrite.write(E)
74     EWrite.close()
75     print('System Message: Encryption Complete')
76 #The lines 73 & 74 writes the encrypted text into a seperate file
77 #labelled in line 47, and closes it, stops the writing to the file.
78
79 def Decryption():
80     DRead = open('plaintext.txt.enc.txt', 'r').read()
81 #This opens the plaintext.txt.enc.txt file and reads it, if the user
82 #did not want to source form a txt file then the code can be replaced
83 #in line 80 by;
84              #print('Enter message to be Decrypted!')
85              #ERead = input()
86     print('Please enter unique key for Decryption!')
87     Dkey = input()
88 #Line 86 & 87 allows the user to input a unique key that is the
89 #important reference to which the code decrypts, thus typing the
90 #key in has to be correct and has to be the same as the key set
91 #during the encryption phase.
92     DMessage = len(DRead)
```

```
93      DKey = Dkey * (1 + DMessage//len(Dkey))
94  #Both the message and key in lines 80 & 87 are now broken down for
95  #their lengths.
96      DWrite = open('plaintext.txt.enc.dec.txt', 'w')
97  #This is the location where the Decrypted text with outputted too.
98  #This allows the code to write into a .txt file.
99      for i in range(DMessage):
100         DPi = ord(DRead[i])
101         Dki = ord(DKey[i]) - 32
102         DCi = DPi - Dki
103 #The above sequences allow for the mathematical formula for
104 #decrypting a message, its is the reverse method to encrypting a
105 #file. Line 100 converts the individual letters of the message into
106 #numbers that corresponds with ASCII 1967 defintions. Lines 101 Does
107 #the following but with the key instead of the message, 32 is then
108 #subtracted but the numbers the individual letters so that the key
109 #is not greater than 126 which is the highest number in the ASCII
110 #1967 defintions. The value of the letters in the message then is
111 #taken away from the value of letters in the key to encrypt the
112 #letter via a number.
113         if DCi < 32:
114             DCi = DCi + 95
115 #If the final value of DCi is greater than 126 (The max limit of the
116 #ASCII 1967 defintions), similiar what happens to the key in line 101.
117         D = chr(DCi)
118 #Line 102 minus the key and the letter togehter to get a single number
119 #the muber is thus changed back into a letter in relation to the
120 #ASCII 1967 defintions. This allows the message in line 80 to be
121 #"encrypted" but replaces the orginal message with the encrypted
122 #message. Which is saved in a .txt file named in line 96.
123         print(DPi, Dki, DCi, D)
124         DWrite.write(D)
125     DWrite.close()
126     print('System Message: Decryption Complete')
127 #The lines 124 & 125 writes the decrypted text into a seperate file
128 #labelled in line 96, and closes it, stops the writing to the file.
129
130 Cipher = getMode()
131 print(Cipher)
```

2 Plaintext

2.1 Encrypted

```
|wpu0+9Vh0%
 ↪   =_a$01Cfy!u'D]_0('I]^~7,SS_|y|JV(0Q,HR]{0+<Zj$0'Bp`y#|S``v0,<Vy$x'I]
^u#7CWy_#!C_(0Y7KRnsx|8p==r|5^m0w$=enu#7=_y%x|SU[#{7BV[#0,<Vydq&BY[&$+9c
yWq,9~yQ|$Seb$|S^i}u&Hdy(y$@p\u0$Cdn0y&Sec}uCS]c{u7HV[#$7=_y#q!B~
```

2.2 Decrypted

```
I've seen things you people wouldn't believe. Attack ships on fire off
 ↪   the shoulder of Orion. I watched C-beams glitter in the dark near
 ↪   the Tannhausser Gate. All those moments will be lost in time, like
 ↪   tears in rain.
```

3 Secret

```
General Kenobi. Years ago, you served my father in the Clone Wars. Now
 ↪   he begs you to help him in his struggle against the Empire. I regret
 ↪   that I am unable to present my father's request to you in person,
 ↪   but my ship has fallen under attack and I'm afraid my mission to
 ↪   bring you to Alderaan has failed. I have placed information vital to
 ↪   the survival of the Rebellion into the memory systems of this R2
 ↪   unit. My father will know how to retrieve it. You must see this
 ↪   droid safely delivered to him on Alderaan. This is our most
 ↪   desperate hour. Help me, Obi-Wan Kenobi. You're my only hope.
```

4 LaTeX Script

```
\documentclass[12pt]{article}
\usepackage[utf8x]{inputenc}
\usepackage[usenames,dvipsnames,svgnames]{xcolor}
\usepackage{amsmath}
\usepackage{graphicx}
\usepackage{float}
\usepackage{dsfont}
\usepackage{amsfonts}
\usepackage[T1]{fontenc}
\usepackage[colorinlistoftodos]{todonotes}
\usepackage[margin=2.5cm,a4paper]{geometry}
\usepackage{listings}
\usepackage{minted}
\usepackage{multicol}
\usepackage{fancyhdr}
\usepackage{cite}
\usepackage{cleveref}
\usepackage{siunitx}
\setlength{\parindent}{0pt}
\newcommand{\deriv}{\mathrm{d}}
\usepackage{color}
\usepackage{hyperref}
\hypersetup{
    colorlinks=true,
    linktoc=all,
    linkcolor=black,
    citecolor=black,
}
\lstset{
    language=R,
    basicstyle=\scriptsize\ttfamily,
    commentstyle=\ttfamily\color{red},
    numbers=left,
    numberstyle=\ttfamily\color{blue}\footnotesize,
    stepnumber=1,
    numbersep=5pt,
    backgroundcolor=\color{white},
    showspaces=false,
    showstringspaces=false,
    showtabs=false,
    frame=single,
    tabsize=2,
    captionpos=b,
    breaklines=true,
    breakatwhitespace=false,
    title=\lstname,
    escapeinside={},
    keywordstyle={},
    morekeywords={}
}

\pagestyle{fancy}
\fancyhf{}
\rhead{PH370 Computing}
\lhead{C4 - Cryptography Assignment}
\rfoot{-\thepage\centering-}

\begin{document}
\begin{titlepage}

\newgeometry{left=1.5in,right=1.5in,top=2.5in,bottom=2.5in}
\newcommand{\HRule}{\rule{\linewidth}{0.5mm}}

\begin{centering}

%------------------------------------------------------------------------
%        HEADING SECTIONS
%------------------------------------------------------------------------

\includegraphics[scale=0.4]{Uni_of_Kent_Logo.png}\\[1cm]

%------------------------------------------------------------------------
%        TITLE SECTION
%------------------------------------------------------------------------

\HRule \\[0.4cm]
\textsc{\large Astronomy, Space Science and Astrophysics}\\[0.4cm]
{\huge \bfseries Cryptography Assignment}\\[0.4cm]
\HRule \\[1.0cm]

%------------------------------------------------------------------------
%        DATE SECTION
%------------------------------------------------------------------------

\textsc{\Large Stage 1 - PH370 Computing}\\[0.5cm]
{\large Monday 19th March 2018}\\[1.0cm]

%------------------------------------------------------------------------
%        AUTHOR SECTION
%------------------------------------------------------------------------

\begin{minipage}{0.625\textwidth}
\centering
```

```
\emph{\large Report Author:} \large Lukasz R Tomaszewski \\ [0.2cm]
\end{minipage}\\[2cm]

\vfill
\end{centering}
\end{titlepage}

%------------------------------------------------------------------------
%------------------------------------------------------------------------
%        CONTENTS
%------------------------------------------------------------------------
%------------------------------------------------------------------------

\newpage
\begin{titlepage}
\begin{tableofcontents}

\end{tableofcontents}
\end{titlepage}

%-----------------------------------------------------------------------
%-----------------------------------------------------------------------
%        PYTHON SCRIPT
%-----------------------------------------------------------------------
%-----------------------------------------------------------------------

\section{Python Script}
\label{Python Script Section}

\inputminted[breaklines,linenos,bgcolor=AliceBlue]{python3}{Encryption.py}

%-----------------------------------------------------------------------
%-----------------------------------------------------------------------
%        PLAINTEXT
%-----------------------------------------------------------------------
%-----------------------------------------------------------------------

\section{Plaintext}
\label{Plaintext Section}

%-----------------------------------------------------------------------
%        ENCRYPTION
%-----------------------------------------------------------------------

\subsection{Encrypted}
\label{Encrypted SubSection}

\inputminted[breaklines,linenos,bgcolor=AliceBlue]{python3}{plaintext.txt.enc.txt}
```

```
%-----------------------------------------------------------------------
%        DECRYPTION
%-----------------------------------------------------------------------

\subsection{Decrypted}
\label{Decrypted SubSection}

\inputminted[breaklines,linenos,bgcolor=AliceBlue]{python3}{plaintext.txt.enc.dec.txt

%-----------------------------------------------------------------------
%-----------------------------------------------------------------------
%        DECODING SCRIPT
%-----------------------------------------------------------------------
%-----------------------------------------------------------------------

\section{Secret}
\label{Secret Section}

\inputminted[breaklines,linenos,bgcolor=AliceBlue]{python3}{secret.txt.dec.txt}

%------------------------------------------------------------------------

\pagebreak
\section{LaTeX Script}
\label{LaTeX Script Section}
\inputminted[breaklines]{tex}{main.tex}

%------------------------------------------------------------------------
%        REFERENCES
%------------------------------------------------------------------------

\end{document}
```