D20128756 -RAHUL

Cryptography Assignment -01

Applications to make the Browser Secure

1. HTTPS Everywhere : it forces the websites to use HTTPS instead of HTTP, encrypting your communication with the websites to protect against the eavesdroppers.
   But now we no-longer need it as it is used by default by majority of the webbrowsers like chrome , Firefox etc.
   - For Chrome browsers, go to Settings > Security and Privacy > Security, scroll to the bottom, and then toggle to "Always use secure connections."
   - For Firefox desktop, go to Settings > Privacy & Security, scroll to the bottom, and then select Enable **HTTPS**-Only Mode.
   - For Safari, make sure you are using Safari 15. HTTPS is upgraded by default without any settings changes needed.
2. Tor Browsers: tor uses onion routing to anonymise web traffic. It conceals the IP address and makes it difficult for websites and third party to track our identity. Particularly uses to maintain high level of anonymity online. **Mostly used by dark web users**
3. Cookie AutoDelete Extension : to automatically delete the cookies as soon as tab is closed to reduce the risk of unwanted tracking. **Goona removed from chrome library soon 'cookie decliner' or 'Tab defender' could be alternative options.**

Applications to Find out who is tracking

1. Privacy Badger: Automatically detects and blocks invisible trackers embedded in websites.

2. Disconnect: shows which websites are tracking your browsing data and blocks them.

Prevention:

1. By blocking third party cookies:

2. using VPN

3. Use Private or incognito mode :

4. regularly clearing cookies and cached files:

CODING:

```
while True:

    print("------------------------------------------------------------")
    print("Welcome to CrytoGraphy World!!")
    print("Select an option below in Integers 1-3 only!!")
    print("1. Caesar Cipher ")
    print("2. Vigenere Cipher ")
    print("3. 2x2 Hill Cipher ")
    print("------------------------------------------------------------")
```

Question 2. Caesar Cipher

Encryption:

```
------------------------------------------------------------
Welcome to CrytoGraphy World!!
Select an option below in Integers 1-3 only!!
1. Caesar Cipher
2. Vigenere Cipher
3. 2x2 Hill Cipher
------------------------------------------------------------
Enter your choice (1-3): 1
You selected Caesar Cipher!
Do you want to encrypt or decrpt?
e/d : e
Encytion Method selected

Enter the key (1 - 26): 6
Enter the text to be encypted: Hi I am Rahul here!!!
CIPHERTEXT : No O gs Xgnar nkxk!!!
```

Decryption:

```
Welcome to CrytoGraphy World!!
Select an option below in Integers 1-3 only!!
1. Caesar Cipher
2. Vigenere Cipher
3. 2x2 Hill Cipher
------------------------------------------------------------
Enter your choice (1-3): 1
You selected Caesar Cipher!
Do you want to encrypt or decrpt?
e/d : d
Decytion Method selected

Enter the key (1 - 26): 6
Enter the text to be decypted: No O gs Xgnar nkxk!!!
PLAINTEXT :  Hi I am Rahul here!!!
```

Question 4: Vigenere Cipher:

```
Welcome to CrytoGraphy World!!
Select an option below in Integers 1-3 only!!
1. Caesar Cipher
2. Vigenere Cipher
3. 2x2 Hill Cipher
------------------------------------------------------------
Enter your choice (1-3): 2
You selected Vigenere Cipher!
Do you want to encrypt or decrypt (e/d):  e
Encryption method Selected

Enter the text to be encypted: explanation
Enter the key:  leg
CIPHERTEXT :  PBVWETLXOZR
Do you want to encrypt or decrypt (e/d):  d
Encytion Method selected

Enter the text to be decypted: PBVWETLXOZR
Enter the key:  leg
PLAINTEXT :  EXPLANATION
Do you want to encrypt or decrypt (e/d):  k
```

Question 3. Caeser Cipher

Output :: ONE VARIATION TO THE STANDARD CAESAR CIPHER IS WHEN THE ALPHABET IS "KEYED" BY USING A WORD. IN THE TRADITIONAL VARIETY, ONE COULD WRITE THE ALPHABET ON TWO STRIPS AND JUST MATCH UP THE STRIPS AFTER SLIDING THE BOTTOM STRIP TO THE LEFT OR RIGHT. TO ENCODE, YOU WOULD FIND A LETTER IN THE TOP ROW

AND SUBSTITUTE IT FOR THE LETTER IN THE BOTTOM ROW. FOR A KEYED VERSION, ONE WOULD NOT USE A STANDARD ALPHABET, BUT WOULD FIRST WRITE A WORD (OMITTING DUPLICATED LETTERS) AND THEN WRITE THE REMAINING LETTERS OF THE ALPHABET. FOR THE EXAMPLE BELOW, I USED A KEY OF "RUMKIN.COM" AND YOU WILL SEE THAT THE PERIOD IS REMOVED BECAUSE IT IS NOT A LETTER. YOU WILL ALSO NOTICE THE SECOND "M" IS NOT INCLUDED BECAUSE THERE WAS AN M ALREADY AND YOU CAN'T HAVE DUPLICATES.

```
------------------------------------------------------------
Welcome to CrytoGraphy World!!
Select an option below in Integers 1-3 only!!
1. Caesar Cipher
2. Vigenere Cipher
3. 2x2 Hill Cipher
------------------------------------------------------------
Enter your choice (1-3): 1
You selected Caesar Cipher!
Do you want to encrypt or decrpt?
e/d :  d
Decytion Method selected

Enter the key (1 - 26): 3
Enter the text to be decypted: RQH YDULDWLRQ WR WKH VWDQGDUG FDHVDU FLSKHU LV ZKHQ WKH DOSKDEHW LV "NHBHG" EB XVLQJ D ZRUG. LQ WKH WUDGLWLRQDO YDULHWB, RQH FRXOG ZULW
H WKH DOSKDEHW RQ WZR VWULSV DQG MXVW PDWFK XS WKH VWULSV DIWHU VOLGLQJ WKH ERWWRP VWULS WR WKH OHIW RU ULJKW. WR HQFRGH, BRX ZRXOG ILQG D LHWWHU LQ WKH WRS URZ DQG V
XEVWLWXWH LW IRU WKH OHWWHU LQ WKH ERWWRP URZ. IRU D NHBHG YHUVLRQ, RQH ZRXOG QRW XVH D VWDQGDUG DOSKDEHW, EXW ZRXOG ILUVW ZULWH D ZRUG (RPLWWLQJ GXSOLFDWHG OHWWHUV)
DQG WKHQ ZULWH WKH UHPDLQLQJ OHWWHUV RI WKH DOSKDEHW. IRU WKH HADPSOH EHORZ, L XVHG D NHB RI "UXPNLQ.FRP" DQG BRX ZLOO VHH WKDW WKH SHULRG LV UHPRYHG EHFDXVH LW LV QR
W D LHWWHU. BRX ZLOO DOVR QRWLFH WKH VHFRQG "P" LV QRW LQFOXGHG EHFDXVH WKHUH ZDV DQ P DOUHDGB DQG BRX FDQ'W KDYH GXSOLFDWHV.
PLAINTEXT :  ONE VARIATION TO THE STANDARD CAESAR CIPHER IS WHEN THE ALPHABET IS "KEYED" BY USING A WORD. IN THE TRADITIONAL VARIETY, ONE COULD WRITE THE ALPHABET ON
TWO STRIPS AND JUST MATCH UP THE STRIPS AFTER SLIDING THE BOTTOM STRIP TO THE LEFT OR RIGHT. TO ENCODE, YOU WOULD FIND A LETTER IN THE TOP ROW AND SUBSTITUTE IT FOR T
HE LETTER IN THE BOTTOM ROW. FOR A KEYED VERSION, ONE WOULD NOT USE A STANDARD ALPHABET, BUT WOULD FIRST WRITE A WORD (OMITTING DUPLICATED LETTERS) AND THEN WRITE THE
 REMAINING LETTERS OF THE ALPHABET. FOR THE EXAMPLE BELOW, I USED A KEY OF "RUMKIN.COM" AND YOU WILL SEE THAT THE PERIOD IS REMOVED BECAUSE IT IS NOT A LETTER. YOU WI
LL ALSO NOTICE THE SECOND "M" IS NOT INCLUDED BECAUSE THERE WAS AN M ALREADY AND YOU CAN'T HAVE DUPLICATES.
```

Question 5. Hill Cipher 2x2:

```
------------------------------------------------------------
Welcome to CrytoGraphy World!!
Select an option below in Integers 1-3 only!!
1. Caesar Cipher
2. Vigenere Cipher
3. 2x2 Hill Cipher
------------------------------------------------------------
Enter your choice (1-3): 3
You selected 2x2 Hill Cipher!
Do you want to encrypt or decrypt (e/d):  e
Encryption method Selected

Enter the text to be encypted: iamhappy
Enter the 4 letter Key:  1021
CIPHERTEXT :  CKBUFUCP
Do you want to encrypt or decrypt (e/d):  d
Decrytion Method selected

Enter the text to be decypted: ckbufucp
Enter the 4 letter key:  1021
PLAINTEXT :  IAMHAPPY
Do you want to encrypt or decrypt (e/d):  exit
```