**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**](https://securityplanner.consumerreports.org/glossary?term=https)-Only Mode.
* For Safari, make sure you are using Safari 15. HTTPS is upgraded by default without any settings changes needed.

1. 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**
2. 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:**

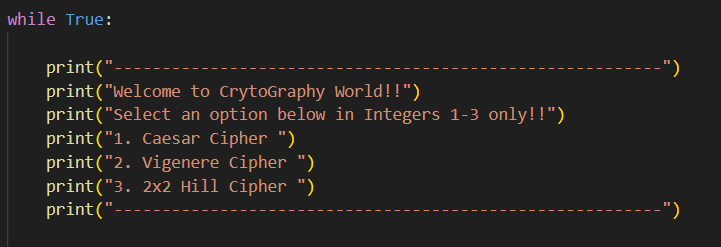
1. By blocking third party cookies:

2. using VPN

3. Use Private or incognito mode :

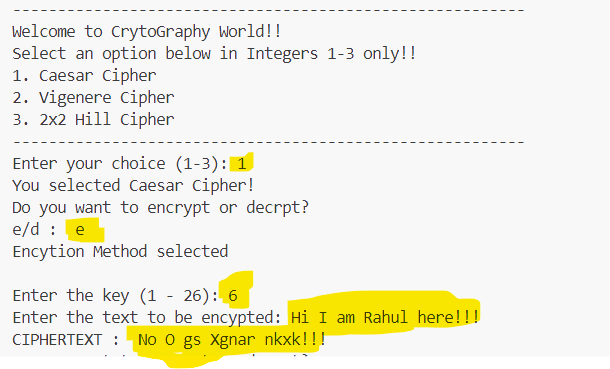
4. regularly clearing cookies and cached files:

**CODING:**

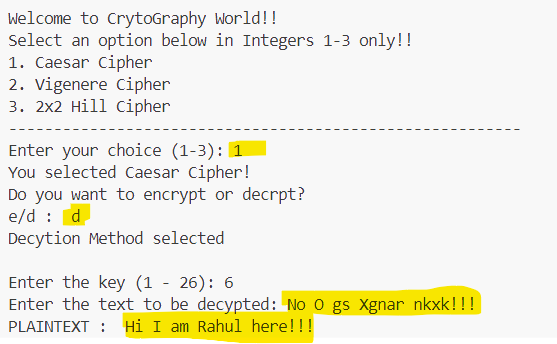


**Question 2. Caesar Cipher**

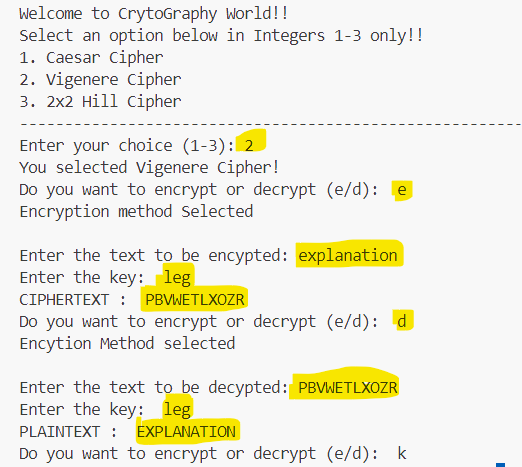
Encryption:



Decryption:

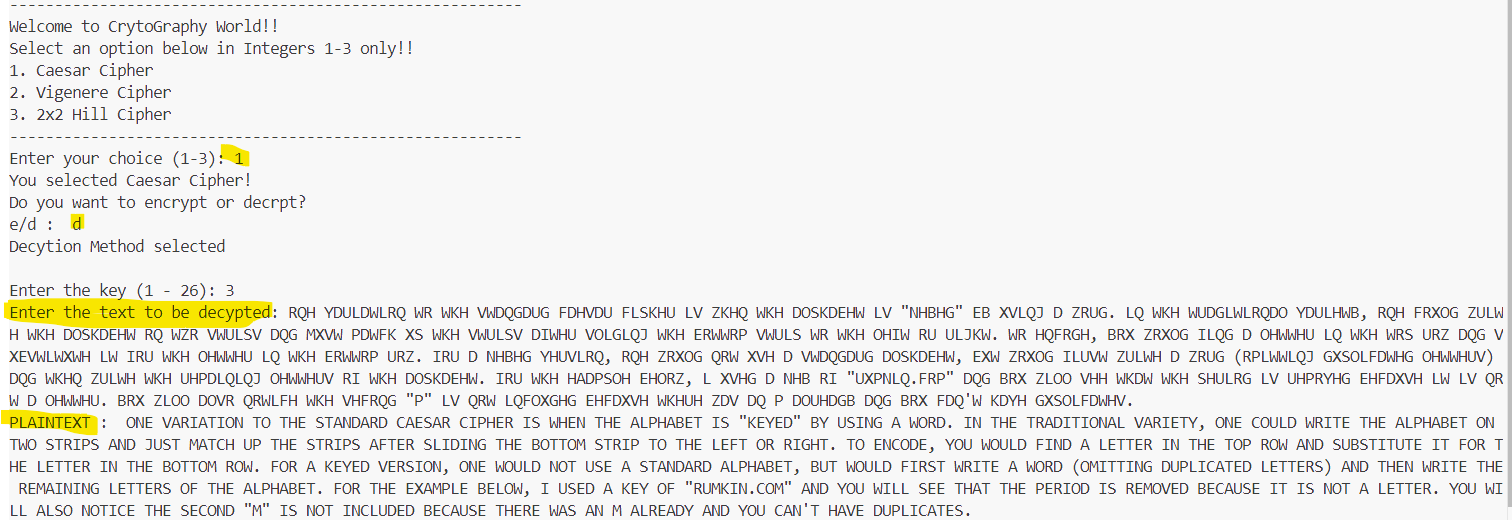


**Question 4: Vigenere Cipher:**



**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.



**Question 5. Hill Cipher 2x2:**

