Homework-1

Questions 1: Explain how Caesar cipher works in a short paragraph. Must answer in your own words. Copying from other sources is unacceptable. (5')

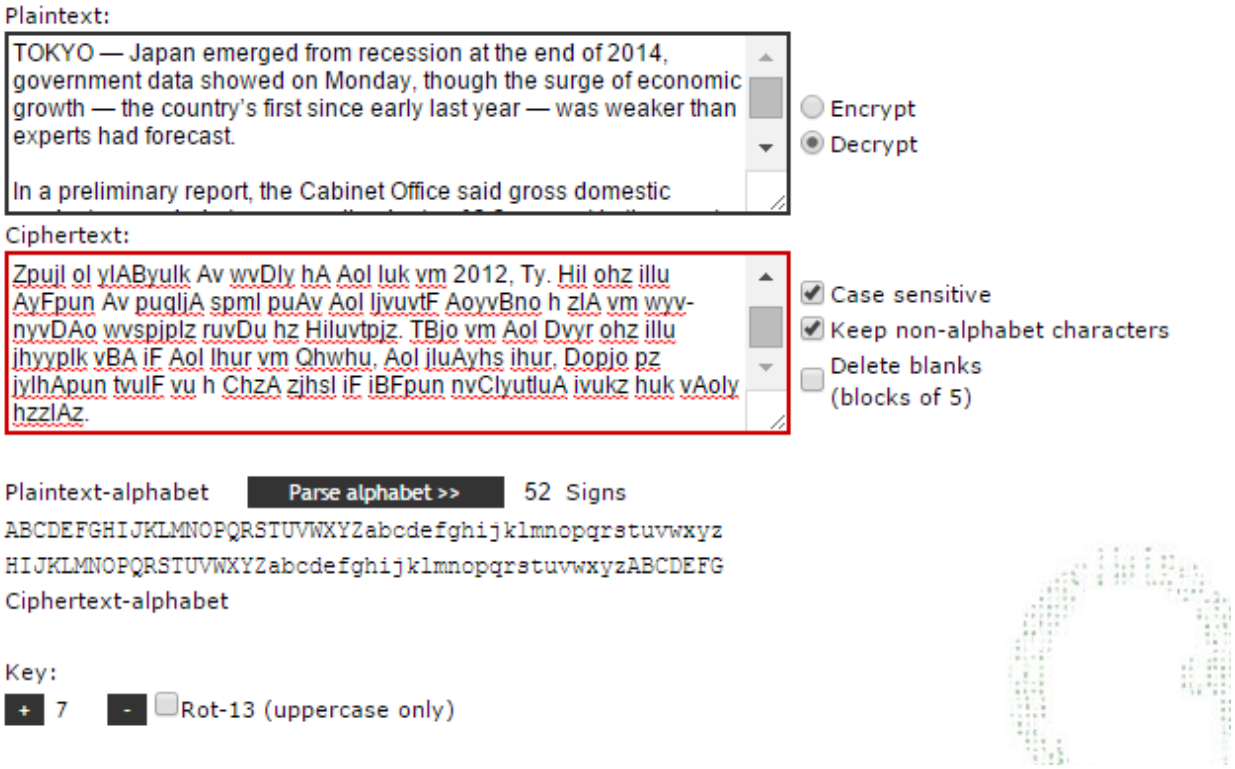
Answer: Caesar cipher is an encryption method for data to be transmitted. In this method each alphabet of the plain text is replaced by an another alphabet which is at a fixed number of positions from it. The number of fixed position is given by us. In our case, we consider key to five, and so the original alphabet is replaced by new alphabet by moving five positions. The text obtained after encryption is known as cipher text which is to be transmitted.

Question 2: Explain what cryptanalysis is and how frequency analysis works in a short paragraph. Must answer in your own words. Copying from other sources is unacceptable. (5')

Answer: Cryptanalysis is a method of decoding or decryption of the encrypted data received without knowing the key. In a frequency analysis s the study of letters or groups of letters contained in a ciphertext in an attempt to partially reveal the message. The method of cryptanalysis is used to decrypt the data by identifying the frequency in occurring of alphabets. In this method it gives the alphabet which has the highest frequency of occurance.

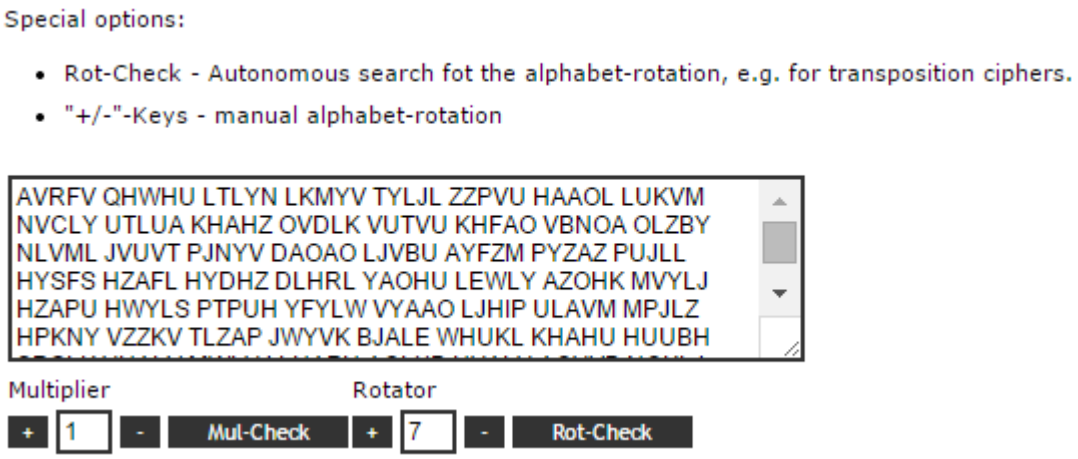
Question 3: Take a screenshot of the encryption information in step 3. – Do not take the whole desktop. Only capture the relevant area as shown below. (5')

Answer:



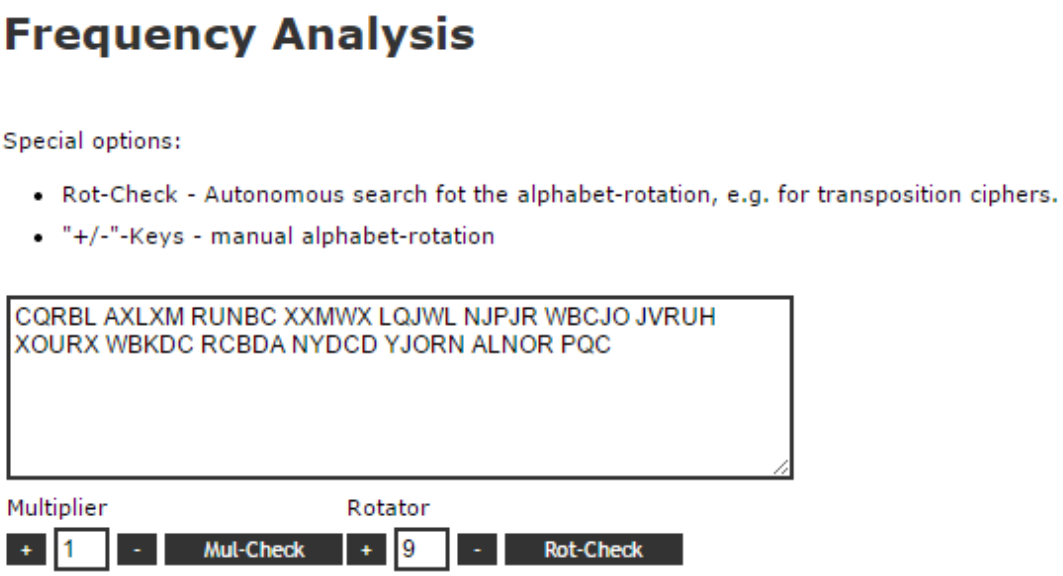
Question 4: Take a screenshot of the frequency analysis information in step 4. (Do not take the whole desktop. Only capture the relevant area as shown below.) Did the frequency analysis find the correct key (need to answer in your own words)? (5')

Answer:



Question 5: Take a screenshot of the frequency analysis in step 5. What is the encryption key that the frequency analysis found (need to answer in your own words)? (5')

Answer:



The encryption key that the frequency analysis found is 9.

Question 6: What is the plaintext obtained in step 6 (copy it from the Web site)? Do you think the decryption is successful? Why? (5')

Answer: The plaintext obtained is "This crocodile stood no chance against a family of lions, but it sure put up a fierce fight."
Yes the decryption was successful as the plain text obtained is in a readable format and it gives some meaning to the sentence.

Question 7: In general, do you think frequency analysis is more likely to find the correct encryption keys from long ciphertexts or short ones? Why? (5')

Answer: Based on my analysis after the trial and error method, I found that the frequency analysis is found correct for long ciphertexts than short ones. This is because the longer the ciphertext, the frequency of finding the occurrence of alphabets is more efficient. Cryptanalysis is the most effective method when compared to other simpler encryption methods.