MIS 578 Homework 1 – Cryptography (35 points)

A list of screen capturing tools is posted in the Assignments area in the course site.

Step 1: CryptTool-Online is a collection of cryptography tools that explain how ciphers and cryptanalysis work. In this project, you will use the Web site to test the Caesar cipher and frequency analysis. Following are instructions on how to use Caesar cipher to encrypt and decrypt data, and how to use frequency analysis to find the key used in a Caesar cipher.

To encrypt data:

1. *Open a Web browser and go to http://www.cryptool-online.org.*
2. *Click on the "Ciphers" tab at the top of the page.*
3. *Click on the link "Caesar / Rot-13" in the left-hand menu.*
4. *Click on the link "test it" toward the top of the page.*
5. *Copy the text you want to encrypt and paste it into the Plaintext box. Delete the default text already in the box before pasting your plaintext.*
6. *Click the "+" or "-" button one or more times to set the encryption key. For example, if you want to use 5 as the encryption key, the number by the "+" button should be 5.*
7. *The data in the Ciphertext box is the encrypted ciphertext.*

To decrypt data:

1. *Go to the Caesar cipher test page as described above.*
2. *Delete the default text already in the Ciphertext box, if any.*
3. *Copy and paste your ciphertext into the Ciphertext box.*
4. *Click the "+" or "-" button one or more times to set the decryption key.*
5. *The data in the Plaintext box is the decrypted text.*

To use frequency analysis:

1. *Open a Web browser and go to http://www.cryptool-online.org.*
2. *Click on the "Cryptanalysis" tab at the top of the page.*
3. *Click on the link "Frequency Analysis" on the left-hand side.*
4. *Click on the link "test it" toward the top of the page.*
5. *Copy and paste your ciphertext into the text box.*
6. *Click the "Rot-Check" button.*
7. *The number in the box below "Rotator" is the key found by the frequency analysis.*

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: Insert your answer here.

With a Caesar cipher, the process begins by placing 2 lines of the alphabet (all in capitals) one after the other. Using these lines as a base point, the process requires the shifting of the second line of the alphabet by a specific number of positions (i.e. the key) to the right. Each letter of the text to be encrypted is replaced with the corresponding letter in the caesar cipher. For example, if the text is "bad" and the key selected is 1, the resulting encryption text will be "cbe", which is one position to the right of each letter in the text (i.e. b=c, a=b, d=e).

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: Insert your answer here.

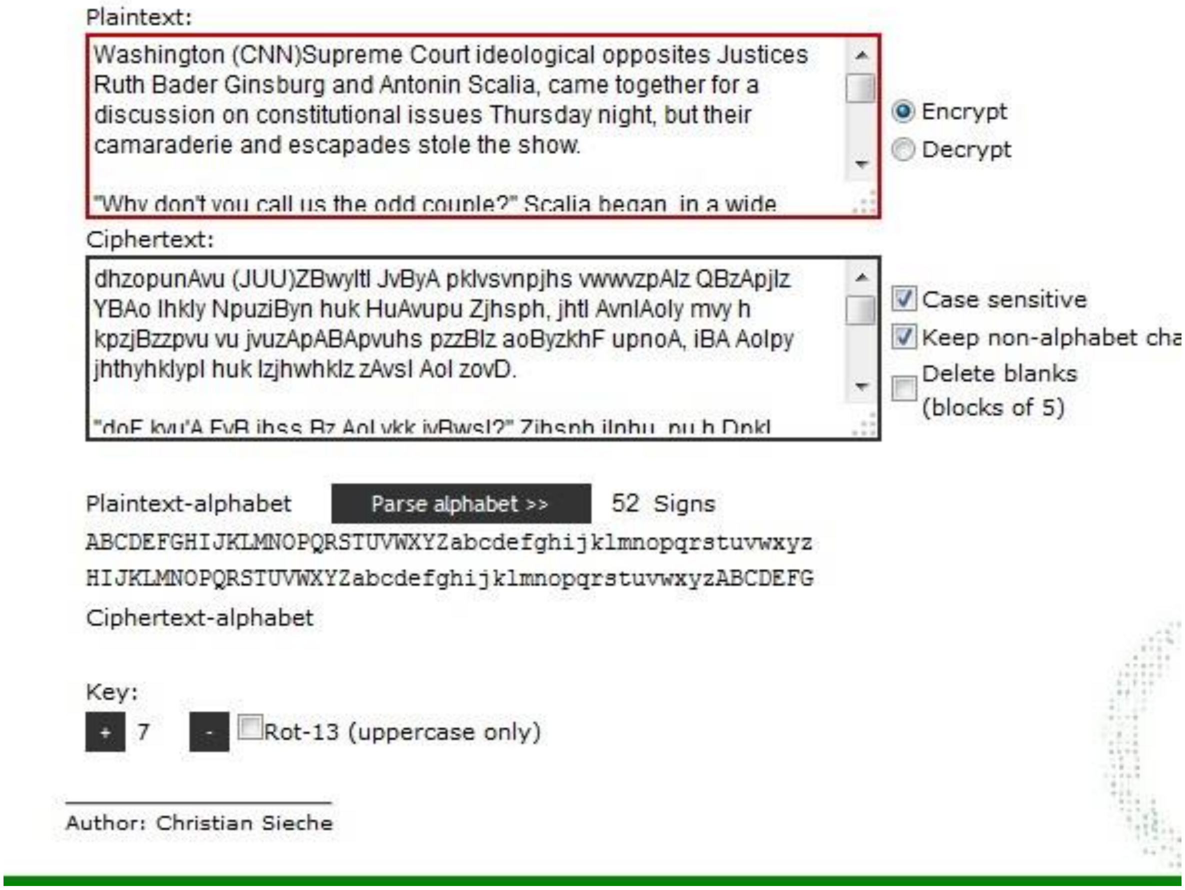
Cryptanalysis is the process of decrypting messages that have been coded with a code system. In cryptanalysis, the key of the system is not known, and therefore, decoding is done by figuring out the key to allow for the decryption of the text. Essentially, the weakness of the system must be identified. Frequency analysis is used to find the weakness of the system by studying the ciphertext to identify the frequency of individual letters or groups of letters. Written language inherently has groups of letters or individual letters that will occur a certain amount of time, and frequency analysis exploits this occurrence.

Step 2: Find a news article from a Web site, such as https://news.google.com.

Step 3: Using 7 as the key, encrypt the article using the Caesar cipher on CrypTool-Online Web site. Copy and paste the ciphertext to a word processing program, such as Notepad, for use in later steps.

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: Insert your answer here.



Plaintext:

Washington (CNN)Supreme Court ideological opposites Justices Ruth Bader Ginsburg and Antonin Scalia, came together for a discussion on constitutional issues Thursday night, but their camaraderie and escapades stole the show.

"Why don't you call us the odd couple?" Scalia began, in a wide

● Encrypt
○ Decrypt

Ciphertext:

dhzopunAvu (JUU)ZBwyltl JvByA pklvsvnpjhs vwwvzpAlz QBzApjlz YBAo Ihkly NpuziByn huk HuAvupu Zjhsph, jhtl AvnlAoly mvy h kpzjBzzpvu vu jvuzApABApvuhs pzzBlz aoByzkhF upnoA, iBA Aolpy jhthyhklypl huk lzjhwhklz zAvsl Aol zovD.

"doF kvu'A FvB ihss Bz Aol vkk jvBwsl?" Zjhsph ilnhu, pu h Dpkl

☑ Case sensitive
☑ Keep non-alphabet cha
☐ Delete blanks (blocks of 5)

ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz
HIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyzABCDEFG

Key:

7

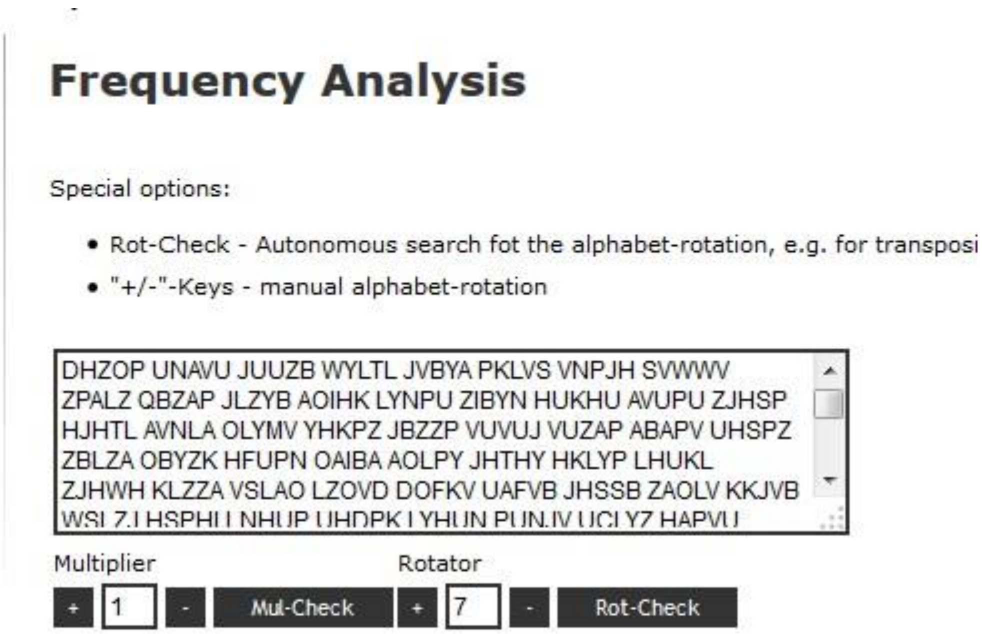
☐ Rot-13 (uppercase only)

Author: Christian Sieche

Step 4: Pretending that you do not know the encryption key used in step 3, use frequency analysis to try to find it from the ciphertext.

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: Insert your answer here.



Frequency Analysis

Special options:

- Rot-Check - Autonomous search fot the alphabet-rotation, e.g. for transposi
- "+/-"-Keys - manual alphabet-rotation

```
DHZOP UNAVU JUUZB WYLTL JVBYA PKLVS VNPJH SVWWV
ZPALZ QBZAP JLZYB AOIHK LYNPU ZIBYN HUKHU AVUPU ZJHSP
HJHTL AVNLA OLYMV YHKPZ JBZZP VUVUJ VUZAP ABAPV UHSPZ
ZBLZA OBYZK HFUPN OAIBA AOLPY JHTHY HKLYP LHUKL
ZJHWH KLZZA VSLAO LZOVD DOFKV UAFVB JHSSB ZAOLV KKJVB
WSLZJ HSPHU NHUP UHDPK LYHUN PUNJV UCLYZ HAPVU
```

Multiplier: 1
Rotator: 7

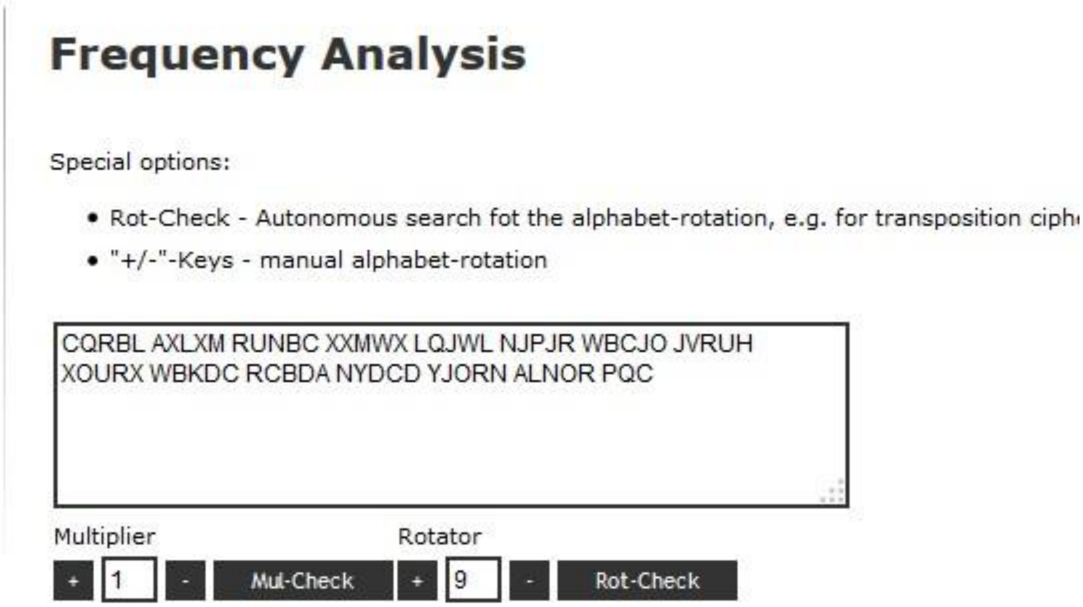
Yes, the frequency analysis found the correct key, which is 7.

Step 5: The following ciphertext is encrypted using Caesar cipher. Use frequency analysis to try to find the encryption key. Ciphertext:

cqrB lAxlxmrun BCxxm wx lqjwln jpjrwBC j ojvruH xo urxwB, kDC rC BDAn yDC Dy j ornAln orpqC.

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: Insert your answer here.



Frequency Analysis

Special options:

- Rot-Check - Autonomous search fot the alphabet-rotation, e.g. for transposition ciph
- "+/-"-Keys - manual alphabet-rotation

```
CQRBL AXLXM RUNBC XXMWX LQJWL NJPJR WBCJO JVRUH
XOURX WBKDC RCBDA NYDCD YJORN ALNOR PQC
```

The key the frequency analysis found is 9. The second line of the alphabet in the cipher is shifted 9 positions to the right, which means the first letter in the text, “C”, is actually “T”.

Step 6: Try to decrypt the ciphertext in step 5 using the key obtained from the frequency analysis. (Note: When doing the decryption, copy and paste the ciphertext from this document rather than from the frequency analysis page because the frequency analysis changes all letters to uppercase.)

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: Insert your answer here.

The plaintext is “This crocodile stood no chance against a family of lions, but it sure put up a fierce fight.” Yes, I believe the decryption was successful because the text is readable and it makes sense from a positional perspective.

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: Insert your answer here.
I think frequency analysis is more likely to find the encryption keys from long ciphertexts. With longer ciphertexts there is more data to determine the frequency of the letters. In shorter ciphertexts, the data can be misleading because there is not enough to compare to the standard letter frequencies found in all written languages.