

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 occurrence.

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:

Plaintext:

TOKYO — Japan emerged from recession at the end of 2014, government data showed on Monday, though the surge of economic growth — the country's first since early last year — was weaker than experts had forecast.

In a preliminary report, the Cabinet Office said gross domestic

Encrypt
 Decrypt

Ciphertext:

Zpujl ol ylAByulk Av wvDly hA AoI iuk vm 2012, Ty. Hil ohz illu AyFpun Av puqljA spml puAv AoI jivutF AoyvBno h zlA vm wyy-nyvDAo wvspjplz ruvDu hz Hiluvtpjz, TBio vm AoI Dvyr ohz illu jhypplk vBA iF AoI ihur vm Qhwhu, AoI ijuAyhs ihur, Dopjo pz jylhApun tvulF vu h ChzA zjhsI iF iBFpun nvClyutluA ivukz huk vAoly hzzIAz.

Case sensitive
 Keep non-alphabet characters
 Delete blanks
(blocks of 5)

Plaintext-alphabet Parse alphabet >> 52 Signs

ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz
HIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ

Ciphertext-alphabet

Key:

+ 7 - Rot-13 (uppercase only)

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:

Special options:

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

AVRFV QHWHU LTLYN LKMYV TYLJL ZZPVU HAAOL LUKVM NVCLY UTLUA KHAHZ OVDLK VUTVU KHFAO VBNOA OLZBY NLVML JVUVT PJNYV DAOAO LJVBW AYFZM PYZAZ PUJLL HYSFS HZAFL HYDHZ DLHRL YAOHU LEWLY AZOHK MVYLJ HZAPU HWYLS PTPUH YFYLW VYAAO LJHIP ULAVM MPJLZ HPKNY VZZKV TLZAP JWYVK BJALE WHUKL KAHU HUUBH

Multiplier Rotator
+ - Mul-Check + - Rot-Check

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:

Frequency Analysis

Special options:

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

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

Multiplier		Rotator	
+ 1 -	Mul-Check	+ 9 -	Rot-Check

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.