Certain letters occur a lot more english language essay

Linguistics, English

In the cipher text, Z is the alphabet that appears the most number of times. Therefore it is presumed that Z is substituted for E. E- 5th letter of the alphabetZ- 26th letter of the alphabetI+k= 265+k= 26k= 21When k= 21, abcdefghijklmnopqrstuvwxyzVWXYZABCDEFGHIJKLMNOPQRSTUFigure 1. 1 Top row depicts the plain text; bottom row depicts the corresponding cipher textUsing Figure 1. 1, the message from the cipher text WPTHJMZNCVMZNVOJIXZ is BUYMORESHARESATONCE.(i) The most frequently occurring letters in this cipher text are letter ‘ g’ and ‘ h’. If ‘ g’ correspond to the most frequently occurring letter in English, ‘ E’,‘ E’- 5th letter of the alphabet, ‘ g‘- 7th letter of the alphabetI+k= 75+k= 7k= 2When k= 2, abcdefghijklmnopqrstuvwxyzCDEFGHIJKLMNOPQRSTUVWXYZABFigure 1. 2 Top row depicts the plain text; bottom row depicts the corresponding cipher textPlaintext will be dqbadfftueeqmeazesmyqmfyupzustfIf ‘ h’ correspond to the most frequently occurring letter in English, ‘ E’,‘ E’- 5th letter of the alphabet,’ h‘- 8th letter of the alphabetI+k= 85+k= 8k= 3When k= 3, abcdefghijklmnopqrstuvwxyzDEFGHIJKLMNOPQRSTUVWXYZABCFigure 1. 3 Top row depicts the plain text; bottom row depicts the corresponding cipher textPlaintext will be fsdcfhhvwggsogcbguoasohawrbwuvhBoth plaintexts do not have any meaning behind the messages. Therefore both ‘ g’ and ‘ h’ does not correspond to the letter ‘ E’ in the plain text.(ii)Figure 1. 4 Cipher text letter frequencies chart(iii) From Figure 1. 4, the longest sequence of low-frequency letters are I, j, k, l, m, n. There are 6 consecutive letters. From Fig 1, we need to obtain 6 consecutive low-frequency letters. They are u, v, w, x, y, z. The letter ‘ u’ is chosen over the letter ‘ a’ because the frequency is higher. Therefore v, w, x, y, z, a are not chosen. For the letter ‘ I’ in the cipher text to correspond to the letter ‘ u’ in plaintext, the length of the cyclic shift will be 14.(iv)Length of the cyclic shift = 14abcdefghijklmnopqrstuvwxyzOPQRSTUVWXYZABCDEFGHIJKLMNFigure 1. 5 Top row depicts the plain text; bottom row depicts the corresponding cipher textUsing figure 1. 5, the message from the cipher text of FSDCFHHVWGGSOGCBGUOASOHAWRBWUVH will be reportthisseasonsgameatmidnight

Question 2

PlaintextMEETMEATSEVENFORTYFIVEKeywordCAGECAGECAGECAGECAGECA Cipher textOEKXOEGXUEBIPFUVVYLMXEFig 2. 1 Cipher text for plaintext ’MEET ME AT SEVEN FORTY FIVE’According to fig 2. 1, the cipher text for text for plaintext ’MEET ME AT SEVEN FORTY FIVE’ will be ‘ OEKX OE GX UEBIP FUVVY LMXE’. Fig 2. 2 Cipher text letter frequencies chartIn Fig 2. 2, there is only one highest letter frequencies that is the letter ‘ e’, whereas in Figure 1. 4, there are 2 letters that have the highest frequencies, letter ‘ g’ and ‘ h’. In Fig 1. 4, there are only 13 different letters used in the plain text, whereas in Fig 2. 2 it would not be possible to derive how many different letters used in the plaintext from the cipher text because of the cipher used. By using the Vigenere cipher, the letter E in the plaintext can be enciphered as different cipher text letters at different points in the message as shown in Fig 2. 1, thus making it difficult for frequency analysis to be used in an attack on this cipher. Repetition of the keyword shows patterns in character frequency that can be analysed and exploited to uncover the keyword. Using frequency analysis, the letter ‘ E’ in the cipher text is the most frequently used. It is matched with the letter ‘ E’ that is the most frequently occurring letter in the

English language. The second letter of the keyword can then be identified as the letter ‘ A’. The problem is using the letter ‘ A’ as part of the keyword, the plaintext will be the same as the corresponding cipher text. The letter ‘ A’ is a trivial key. If the keyword used is the same length as or greater than the length of the plaintext, the weakness in (d) would be circumvented. The length of the plaintext in this question is 22 letters. Therefore a different choice of keyword would require a keyword that contains 22 letters or more. The disadvantages are the keyword would be difficult for both parties to remember, thus making it very likely that they would write it down somewhere, leaving the secrecy of the keyword in jeopardy. The keyword might be a combination of English words or phrases. It would be harder for the attacker to guess the characters of the plaintext message from the keyword, if each letter is randomly generated and only used once.

Question 3

The distance between the occurrences of the sequence ‘ Y P I’ is 50 letters. 3-letter sequenceDistance between occurrencesYPI50SBM20BWP45Fig 3. 1 3-letter sequence and its respective distance in letters. The greatest common divisor between 50, 20, and 45 is 5. Therefore k= 5. Fig 3. 2 Frequencies of the 1st letter in the cipher textFrom Fig 3. 2, the longest sequence of low-frequency letters are z, a, b, c, d, e, f. There are 7 consecutive letters. From Fig 1, we need to obtain 7 consecutive low-frequency letters. They are u, v, w, x, y, z, a. For the letter ‘ z’ in the cipher text to correspond with letter ‘ u’ in the plaintext, the length of the cyclic shift will be 5. Fig 3. 3 Frequencies of the 2nd letter in the cipher textFrom

Fig 3. 3, the longest sequence of low-frequency letters is d, e, f, g, h. There are 5 consecutive letters. From Fig 1, we need to obtain 5 consecutive low-frequency letters. They are v, w, x, y, z. For the letter ‘ d’ in the cipher text to correspond with letter ‘ v’ in the plaintext, the length of the cyclic shift will be 8. Fig 3. 4 Frequencies of the 3rd letter in the cipher textFrom Fig 3. 4, the longest sequence of low-frequency letters are y, z, a, b, c, d. There are 6 consecutive letters. From Fig 1, we need to obtain 6 consecutive low-frequency letters. They are u, v, w, x, y, z. For the letter ‘ y’ in the cipher text to correspond with letter ‘ u’ in the plaintext, the length of the cyclic shift will be 4. Fig 3. 5 Frequencies of the 4th letter in the cipher textFrom Fig 3. 5, there are 4 longest sequences of low-frequency letters. They are ‘ a, b, c’,’ g, h, I’, ‘ q, r, s’ and ‘ u, v, w’. Therefore using the low-frequency letters to identify the length of the cyclic shift is not possible. Instead, the letter frequency data in Fig 3. 5 is used to find the length of the cyclic shift. In Fig 3. 5, the letter ‘ p’ is the most frequently occurring letter. From Fig 1, the most frequently occurring letter in English is the letter ‘ e’. For the letter ‘ p’ in the cipher text to correspond with letter ‘ e’ in the plaintext, the length of the cyclic shift will be 11. Fig 3. 6 Frequencies of the 5th letter in the cipher textFrom Fig 3. 6, there are 2 longest sequences of low-frequency letters. They are ‘ k, l, m, n’ and ’x, y, z, a’. Therefore using the low-frequency letters to identify the length of the cyclic shift is not possible. Instead, the letter frequency data in Fig 3. 6 is used to find the length of the cyclic shift. In Fig 3. 6, the letter ‘ h’ is the most frequently occurring letter. From Fig 1, the most frequently occurring letter in English is the letter ‘ e’. For the letter ‘ h’ in the cipher text to correspond with letter ‘ e’ in the plaintext, the length of the cyclic shift will be 3. The five letters obtained above are combined into one keyword: FIELD. The decryption process of the cipher text will be as shown below. Cipher textYPINRRXEYBNAGZPRQXEHIBSDHKeywordFIELDFIELDFIELDFIELDFIELDPlaintextTHECOMPANYISCOMMITTEDTOSECipher textQTMYJNBWPQYQVPRUMVLWNWRTQKeywordFIELDFIELDFIELDFIELDFIELD PlaintextLLINGITSENTIREOPERATIONINCipher textYPIPDXBIFUTXILQXCFNRSBMYHKeywordFIELDFIELDFIELDFIELDFIELDPlaintextTHEEASTEUROPEANSUBCONTINECipher textSBWPFWMGJLXMWDHSBMLOGMJZUKeywordFIELDFIELDFIELDFIELDFIELDPlaintextNTSECRECYISESSENTIALBEFORCipher textJBLPWJIQXHJBWKeywordFIELDFIELDFIEPlaintextETHETEAMMEETSFig 3. 7 Decryption of cipher text using the keyword FIELDFrom Fig 3. 7, the original plaintext is THE COMPANY IS COMMITTED TO SELLING ITS ENTIRE OPERATION IN THE EAST EUROPEAN SUBCONTINENT SECRECY IS ESSENTIAL BEFORE THE TEAM MEETS