CSEC 507: Applied Cryptology
Homework 1
(Deadline 1 December 2022 09:40)

1 Caesar's Cipher (20 points)

1. Encrypt the following plaintexts using the Caesar's cipher where k denotes the number of left shifts in the English alphabet (YOU DO NOT NEED TO WRITE A CODE FOR THIS QUESTION, do it by hand):
   (a) CYBERSECURITY, $k = 1$
   (b) CYBERSECURITY, $k = 2$
   (c) CYBERSECURITY, $k = 3$
   (d) CYBERSECURITY, $k = 25$
2. You capture the following ciphertexts which are obtained from Caesar's cipher. Obtain the plaintexts and find the corresponding k (YOU DO NOT NEED TO WRITE A CODE FOR THIS QUESTION, do it by hand):
   (a) NCCYVRQPELCGBYBTL
   (b) ECGUCTEKRJGT

2 XOR Operation (20 Points)

1. Compute the following XOR operations (preferably by hand) where $\bar{}$ represents the bitwise complement and $_x$ denotes hexadecimal values (e.g. $\overline{0123}_x = FEDC_x$). Do it by hand, you can verify your results by writing some code (rightmost bit is the least significant bit):
   (a) $FFFFFFFF_x \oplus 11111111_x$
   (b) $11111111_x \oplus 22222222_x$
   (c) $ABCDE_x \oplus A87CA4_x$
   (d) $\overline{FFFFFFFF}_x \oplus 11111111_x$
   (e) $\overline{FFFFFFFF}_x \oplus \overline{11111111}_x$

3 Frequency Analysis (60 Points)

1. (15 POINTS) Compute the frequency analysis of the languages English and Turkish using long enough documents written in these languages. Provide (electronically) the documents you used for this analysis and provide frequencies of each letter. If you write a code for this question, also provide your source code. If not, mention how you did the counting.

   For each language, provide your frequency analysis result sorted with respect to the frequency ratios like follows (here the ratio is the number of occurrences of a letter divided by the total number of letters that appear in that document):

Letter	Count	Ratio
E	150535	0.12345
A	9535	0.05487
.	.	.
.	.	.
.	.	.
Y	1053	0.00545

If you solve this homework by writing a code, do not forget to submit your source code. However, you are allowed to use any software to count letters so you do not have to write a code for this homework. Do not forget to explain which documents (submit if possible) and which software you used for this question.

HINT: You can convert your document to a TXT file and open it using a modern browser like Chrome or Firefox. Count the occurrences of each letter simply by first searching the letter ”a” in the document, then ”b”, and so on. Your browser should tell you the number of occurrences.

2. (15 POINTS) Using your frequency analysis, decrypt the ciphertext provided in *turciphertext.html* which is assumed to be written in Turkish (numbers or symbols are not encrypted) and provide the key. Note that directly using your frequency analysis results might **not** give you the correct plaintext. However, you can obtain the plaintext by trial and error. You **must** obtain the key that provides the correct plaintext. Explain in detail how you overcame this problem and obtained the plaintext (Do not use a tool or Google. Obtain the plaintext yourself and enjoy your first cryptanalysis!!!).

3. (15 POINTS) Using your frequency analysis, decrypt the ciphertext provided in *engciphertext.html* which is assumed to be written in English (numbers or symbols are not encrypted) and provide the key. Note that directly using your frequency analysis results might **not** give you the correct plaintext. However, you can obtain the plaintext by trial and error. You **must** obtain the key that provides the correct plaintext. Explain in detail how you overcame this problem and obtained the plaintext (Do not use a tool or Google. Obtain the plaintext yourself and enjoy your first cryptanalysis!!!).

4. (15 POINTS) Did your frequency analysis results completely match with the keys? We do not expect that they do. Provide at least 5 reasons why your the frequencies of the letters that you calculated in the first question do not match with the frequencies of the letters of the obtained plaintexts.