THE UNIVERSITY of NEW ORLEANS

CSCI 4130/5130 INTRODUCTION TO CRYPTOGRAPHY

Spring 2026

DUE: January 29, 11:59 pm

PART 1 [50 points]

Alice is a student in our class. She also happens to be a movie actor. She wanted to share the plot of one of her movies with Bob. Although she knew that the substitution cipher was not completely secure, she still wanted to use it as she had an urgent need to send this message. She could not wait for the end of the course to get to know more secure ciphers. She did some brief research about the tools that can solve substitution cipher. Unfortunately, she discovered that there are many such online tools that can automatically solve substitution ciphers (https://www.guballa.de/substitution-solver and https://www.dcode.fr/frequency-analysis).

So, she tried to slightly strengthen the substitution cipher instead of following the textbook approach as it is.

Instead of substituting just the letters, she also used the “punctuation letters” that were in her text as part of the substitution mapping. To be specific, these are the all the letters that she had a mapping for:

abcdefghijklmnopqrstuvwxyz "',-.;

Note how she has a mapping for 7 special characters: space (right after z), double quote, single quote, comma, hyphen, period and semi-colon.

So, she now has 33 characters that will all be substituted. This change improved the key space size to 33! (roughly equal to 2^{122}) keys and thus strengthened the cipher!

More importantly for Alice, most of the online tools didn’t seem to work as well anymore after using this version of the cipher. This provided some comfort to her and she went on to send a message to Bob. We were able to get hold of the encrypted text that she sent: “cipher.txt” file uploaded to Canvas on the assignment page.

Now, break this cipher and find the plain text as well as the correct key used for encryption. The encryption key should be represented as a single line of text where each character denotes the character that it replaces. An example key is the following (but, this is not the correct key).

;q'oc.ikbaugjtf,vn"yl -ehdrxzwmsp

You should submit the **plain text, encryption key** as well as **any code** that you wrote as part of the cryptanalysis.

- It’s also OK to do the entire cryptanalysis in a manual manner (without any programming). If that’s the case, please submit **a brief write-up** about how you arrived at the answer.
- You can also use any of the available online tools to find the solution. If that’s the case, please **mention the tool** that you used in the write-up and also **how you used it** to arrive at the answer.

- Here are some helpful tips about how you can crack a substitution cipher (apart from what we've seen in the textbook):

  https://www.simonsingh.net/The_Black_Chamber/hintsandtips.html

PART 2 [50 points]

Q1-) [10 points]

We received the following ciphertext which was encoded with a shift cipher (Caesar Cipher):

xultpaajcxitltlxaarpjhtiwtgxktghidhipxciwtvgtpilpitghlxiwiwtxgqadds.

a. Perform an attack against the cipher based on a letter frequency count: How many letters do you have to identify through a frequency count to recover the key? What is the cleartext?

b. Who wrote this message?

Q2-) [16 points]

We now consider the relation between passwords and key size. For this purpose we consider a cryptosystem where the user enters a key in the form of a password.

a. Assume a password consisting of 8 letters, where each letter is encoded by the ASCII scheme (7 bits per character, i.e., 128 possible characters). What is the size of the key space which can be constructed by such passwords?

b. What is the corresponding key length in bits?

c. Assume that most users use only the 26 lowercase letters from the alphabet instead of the full 7 bits of the ASCII-encoding. What is the corresponding key length in bits in this case?

d. At least how many characters are required for a password in order to generate a key length of 128 bits in case of letters consisting of

  d1. 7-bit characters?

  d2. 26 lowercase letters from the alphabet?

Q3-) [8 points]

What is the multiplicative inverse of 5 in Z_{11}, Z_{12}, and Z_{13}?

Q4-) [16 points]

An obvious approach to increase the security of a symmetric algorithm is to apply the same cipher twice, i.e.:

$$y = e_{k2}(e_{k1}(x))$$

As is often the case in cryptography, things are very tricky and results are often different from the expected and/ or desired ones. In this problem we show that a double encryption with the affine cipher is only as secure as single encryption!

Assume two affine ciphers $e_{k1} = a_1x+b_1$ and $e_{k2} = a_2x+b_2$.

a. Show that there is a single affine cipher $e_{k3} = a_3x+b_3$ which performs exactly the same encryption (and decryption) as the combination $e_{k2}(e_{k1}(x))$.

b. Find the values for a_3, b_3 when $a_1 = 3$, $b_1 = 5$ and $a_2 = 11$, $b_2 = 7$.

c. For verification:

(1) encrypt the letter K first with e_{k1} and the result with e_{k2},

(2) encrypt the letter K with e_{k3}.

d. Briefly describe what happens if an exhaustive key-search attack is applied to a double-encrypted affine ciphertext. Is the effective key space increased?