**Applied Crypto**

**CS-GY 6903 CF01/CF02**

**Insights from Classic Ciphers and Enigma Machine**

**Instruction**

This is an individual project. Do three out of four problems. Three best points will be added to your final points.

Submission

1. Project report using PDF format **(**proj1\_your\_name.pdf**)**
   * Ensure that your submission is clear, well-organized, and comprehensively covers all aspects of the assignment.
   * Use appropriate headings and mark the problem numbers clearly for easy reference.
   * May include codes in the report. Students still need to submit the Jupyter Notebook.
2. Jupyter Notebook (proj1-Your\_name.ipynb)
   * Students shall use Jupyter Notebook for the coding.
   * The Jupyter Notebook file shall contain all the coding solutions. It should be well-commented, indicating what each segment does, and should correspond to the problems as numbered in the assignment.
   * Ensure that the notebook is executable without errors and that the outputs of your code are visible. For example, add all the pip install statements in a code box at the top of your ipynb notebook if they are not installed already in the CA’s machine.

If students use Jupyter Notebook to do all the work includes those discussion/essay problems. They still need to submit the exported PDF file.

It is OK students use colab or any other cloud-based development environments for their work. When they submit the work, they need to submit the actual notebook code (.ipynb), not the link to their project.

**Grading rubrics**

(CA will grade all the problems you do and select three best three as final project point)

|  |  |  |
| --- | --- | --- |
|  | Point | Expectations |
| Problem 1 (Vigenère cipher) | 4 |  |
| a | 2 | Show the work to do encryption correctly |
| b | 2 | Show the work to do encryption correctly |
| Problem 2 (Affine Cipher) | 4 |  |
| a | 1 | Find the formula correctly |
| b | 1 | Find the cipher correctly |
| c | 2 | Solve the decryption, show your work |
| Problem 3 (Freq Analysis) | 4 |  |
| a | 1 | Get the formula correctly |
| b | 3 | Decrypt the message correctly |
| Problem 4 (Enigma Machine) | 4 |  |
| a | 1 | Write the formula accurately |
| b | 1 | Correct observation |
| c | 2 | Write the code, show the result, follow code best practice. |

**Problem 1: Vigenère cipher**

(a) Encrypt the message using the Vigenère cipher with the given key, k = ‘apple’ to the message, m = ‘theclassistough’ to produce the ciphertext. Then (b) decrypt the ciphertext back to retrieve the original plaintext. Show your work.

**Problem2: Affine Cipher**

The Affine cipher is a type of monoalphabetic substitution cipher that employs modular arithmetic to encrypt the letters of a message. The encryption formula is c = (a \* p + b) mod n, where 'p' is the plaintext letter, 'c' is the ciphertext letter, 'n' is the modulus. 'a' and 'b' are keys, and 'a' must be chosen such that 'a' and 'n' are coprime (relatively prime). In this cipher, each letter of the plaintext is converted into an integer, for example, A=0, B=1, C=2, and so on.

a) What is the size of key space for a fixed modular n? Students can use the notation of the Euler's totient Φ(n) which is defined as the number of integers less than n and relative prime to n.

b) Imagine you're a cryptographer tasked with sending a secure message using the Affine Cipher. Your message consists only of capital letters, and you've decided to use the encryption formula *c* = 5*p*+9 mod 26 and do it manually. What is the ciphertext for the plaintext “CRYPTOISFUN”?

c) Eve has intercepted a ciphertext “QJKESREOGHGXXREOXEO” and, through her intelligence sources, discovered that it’s encrypted using an Affine Cipher. She also has limited information about the encryption process: the letter 'T' is encrypted to 'H' and 'O' to 'E'. With this knowledge, she aims to decrypt the message. Your challenge is to help Eve by developing a method to find the decryption function of the Affine Cipher using the given information. You do it manually. Show your work.

**Problem 3 Frequency Analysis**

Alice has crafted a message for Bob using a simple substitution cipher. The encrypted message, segmented is "TNFOS FOZSW PZLOC GQAOZ WAGQR PJZPN ABCZP QDOGR AMTHA RAXTB AGZJO GMTHA RAVAP ZW", where spaces are not part of the original encryption and are added only for convenience. Eve, who has intercepted the message, knows that the word "liberty" appears somewhere in the plaintext.

a) Calculate the Size of the Key Space. Explain how the key space is calculated and its implications for the cipher's security.

b) Given Eve's knowledge that the word "liberty" is in the plaintext, devise a strategy to decrypt the message. This task requires analyzing the ciphertext, making educated guesses, and testing hypotheses about the cipher's key. Your goal is to uncover the original message sent by Alice to Bob. You can solve it using any resources you have. A detailed explanation of your method is required.

**Problem 4: Understanding and Analyzing the Enigma Machine**.

The Enigma machine, used extensively during World War II, is a fascinating example of early mechanical encryption technology. With its complex system of rotors, reflectors, and plugboards, it offered a then-unprecedented level of security. Your task involves understanding the Enigma's encryption process, estimating the size of its key space, and performing cryptanalysis on a given ciphertext.

a) Assess and calculate the size of the key space of the Enigma machine. Consider all elements that contribute to the key space: rotor wiring, ring settings, rotor stepping, reflector choices, plugboard configurations, and the initial position of rotors. We assume 3 out of 5 rotors and 10 pairs used in plugboard (check class slides)

b) Refer to the manual at <https://py-enigma.readthedocs.io/_/downloads/en/latest/pdf/> Here is one code sample for enigma machine. Test it with different configurations. Just in case, you know you need to install the package py-enigma. A better approach is to ask if a required package is installed or not.

Write your observations on the outcome when the plaintext has numbers or special characters.

from enigma.rotors.rotor import Rotor  
from enigma.plugboard import Plugboard  
from enigma.machine import EnigmaMachine  
  
rL = Rotor('my rotor1', 'EKMFLGDQVZNTOWYHXUSPAIBRCJ', ring\_setting=0, stepping='Q')  
rM = Rotor('my rotor2', 'BDFHJLCPRTXVZNYEIWGAKMUSQO', ring\_setting=5, stepping='V')  
rR = Rotor('my rotor3', 'ESOVPZJAYQUIRHXLNFTGKDCMWB', ring\_setting=10, stepping='J')  
  
reflector = Rotor('my reflector', 'YRUHQSLDPXNGOKMIEBFZCWVJAT')  
  
pb = Plugboard.from\_key\_sheet('AK BZ CG DL FU HJ MX NR OY PW')  
  
machine = EnigmaMachine([rL, rM, rR], reflector, pb)  
  
machine.set\_display('UPS') # set rotor positions or use its default  
position = machine.get\_display() # read rotor position  
print(position)  
  
# Encrypt A letter  
#print(machine.key\_press('C'))  
# Encrypt a text  
print(machine.process\_text('Enigma machine is powerful for Q'))

c) The codebreakers at Bletchley Park have intercepted a ciphertext “WVUVJCSQBFLEJGFNIZNIGYGOCWSUVNCIIIA” which they know corresponds to the plaintext “ATTACKXATXXXXXXATXATLANTICXZXISLAND”. It sounds like “ATTACKxATxxxxxx ATLANTICxZxISLAND”. Your challenge is to determine the initial rotor display position (code line machine.set\_display(xxx) ) used to encrypt this message programmatically. Use your code to simulate the Enigma machine and discover the initial settings.