Applied Crypto

CS-GY 6903 CF01/CF02

Fun from the Classic Ciphers

This project is to focus on the fun from classical ciphers. For each problem, students need to explain the mentioned ciphers briefly and propose the way to crack it to get plaintext. Please follow the team project guidelines from the course outline.

Problem1: Affine Cipher

Affine cipher is a type of monoalphabetic substitution cipher that uses modular arithmetic to encrypt the letters of a message. The mathematical module formula is $c = ap + b \bmod n$ where input p is plaintext, the output c is the ciphertext, n is a modular integer, a and b are non-negative integers less than n, a and n are relatively prime (to do decryption). We assume all the letters are encoded to unique integers.

1a) Describe affine cipher in more detail.

1b) What is the size of key space for a fixed integer n? Hint: Use Euler's totient $\Phi(n)$

1c) Let us assume the plaintext is made of 26 capital letters only. So, the n=26.
Given the affine cipher $c = 5p + 9 \bmod 26$, what is the ciphertext for the plaintext "CRYPTOISFUN". Here we remove the space because its domain is 26 letters.

1d) Eve has the ciphertext "**QJKESREOGHGXXREOXEO**". She magically knows the cipher is an affine cipher and the letter T is encrypted to H and O to E. Recover the decryption function and decipher the message. Students can solve it manually. They can also solve it by a computer program. They both shall give the same results. Remember, the code shall be more general, not just in this case. Submit both results.

1e) What is the affine formula if we want to include the space and little letter case in the encde set?

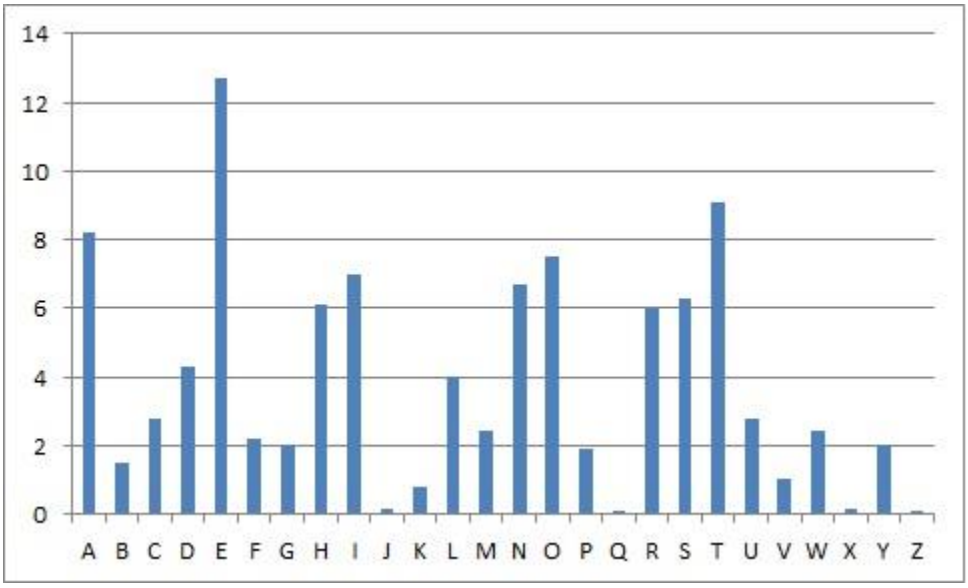
Problem 2 Frequency Analysis

Alice uses a simple substitution cipher to send her message to Bob. It reads as "**TNFOS FOZSW PZLOC GQAOZ WAGQR PJZPN ABCZP QDOGR AMTHA RAXTB AGZJO GMTHA RAVAP ZW".** There shall be no space in the ciphertext. We add it here every five letters just for ease of reading and processing. Eve gets the ciphertext and she also heard the word "liberty" appears in the plaintext.

2a) Describe the substitution cipher.

2b) What is the size of key space?

2c) Use the frequency of English letters as reference to recover the plaintext. We can do it manually. Optionally, we can do it by coding. It is a bit of a challenge. It is doable.



2d) (optional) The following message is from a Vigenère cipher with a 3-letter English keyword: "**CTMYR DOIBS RESRR RIJYR EBYLD IYMLC CYQXS RRMLQ FSDXF OWFKT CYJRR IQZSM X".** Recover the plaintext. Again, space is added later every five letters just for ease of processing. There is no space in the original ciphertext.