Cryptography and Quantum Cryptography
Homework 1

Yvonne Akinyi Amugaga
Neptune: Y2Q07H
Msc Applied Mathematics

February 28, 2026

0.1 Selected Text

The selected Spanish four-line poem is:

> Bajo el cielo de España diremos “sí, acepto”,
> el tres de octubre sellamos nuestro amor perfecto.
> Con el alma entrelazada y el corazón encendido,
> me caso con el amor de mi vida, mi destino elegido.

Spanish Alphabet Used

A B C D E F G H I J K L M N Ñ O P Q R S T U V W X Y Z

This alphabet contains 27 letters.

0.2 Normalization

All letters were converted to uppercase. Accented characters were replaced and all non-alphabetic characters were removed.

Normalized Plaintext:

BAJOELCIELODEESPANADIREMOSSIACTO
ELTRESDOCTUBRESELLAMOSNUESTROAMORPERFECTO
CONELALMAENTRELAZADAYELCORAZONENCENDIDO
MECASOCONELAMORDEMIVIDAMIDESTINOELEGIDO

0.3 Caesar Cipher

A shift of 3 was used.

$$C = (P + 3) \mod 27$$

Encrypted text:

EDMRHÑFLHÑRGHHVSDQDGLUHORVVLDFHSWRHÑWUHV

GHRFWXEUHVHÑÑDORVPXHVWURDORUSHUIHFWRFRPH
ÑDÑODHPWUHÑDCDGDBHÑFRUDCRPHPFHPGLGROHFDV
RFRPHÑDORUGHOLYLGDOLGHVWLPRHÑHJLGR

0.4 Vigenere Cipher

Keyword used: **AMOR**

$$C_i = (P_i + K_i) \mod 27$$

Encrypted text:

BMXGEWQZEWDUEPHHAZOUIDSDOEHZAÑSHTASCTDSK
DPDTTGPJEESCLMAGSYJVSFGGAXDJPPGWEÑIGCABV
LMZDAPBLRPZRZMRRYPZTODOQOYSECPBUIODDEÑOK
OÑDEEWODODRVMTKZDMAZDPHLIYDVLPUZDA

0.5 Enigma Encryption

A simplified Enigma machine was implemented in Python using:

- Three rotors
- One reflector
- Rotor stepping mechanism

Encrypted text:

BAIBIOGZFWSHINIBEZNOIWGCTCJYQXTFHHMCOIUÑ
TUÑSÑZQZCPEMKDTÑQMSDQTUBÑVODHDOVUAKUBEFD
DNFXIZMDÑYVSRUJMSOVNBHNMSPEBCXEPWNBPSGDU
KTOCKAGBYZRRXXKWQVWPRKFHIYBYQNUÑOE

0.6 Frequency Analysis

Letter frequencies were computed for:

- Original text
- Caesar cipher text
- Vigenere cipher text
- Enigma cipher text

0.6.1 Original Text Statistics

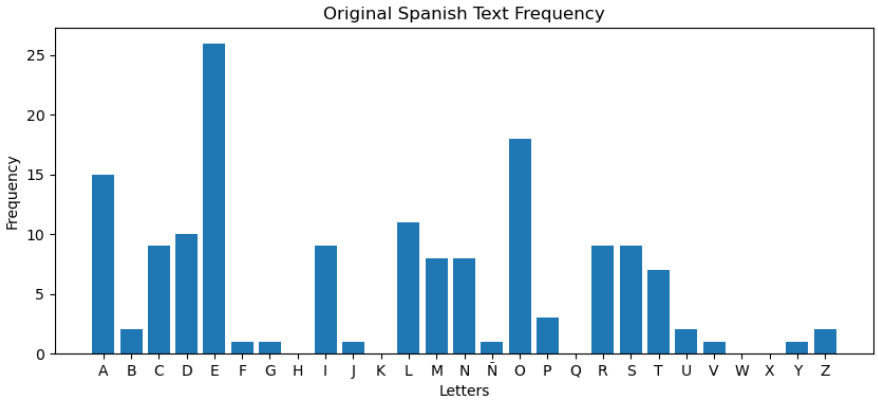

Figure 1: Letter frequency of the original Spanish text

Observation:

The letters E, A, O, S, R and N appear most frequently, which corresponds to the known statistical properties of Spanish.

0.6.2 Caesar Cipher Statistics

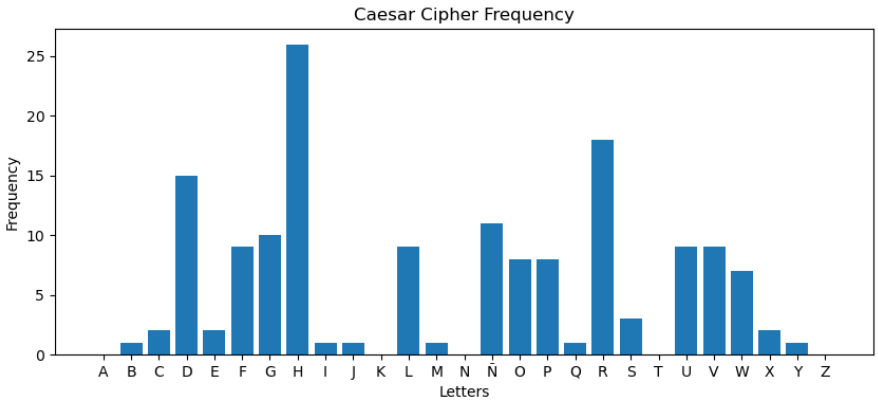

Figure 2: Letter frequency after Caesar encryption

Observation:

The distribution remains identical to the original but shifted cyclically. The statistical structure of the language is still clearly recognizable.

0.6.3 Vigenere Cipher Statistics

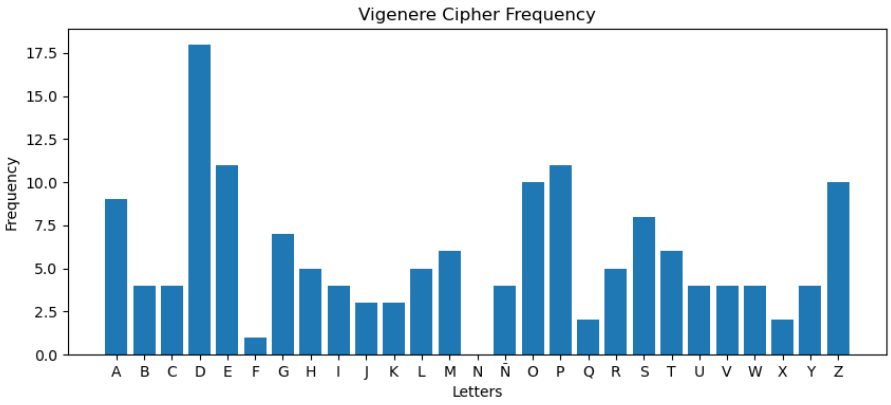

Figure 3: Letter frequency after Vigenere encryption

Observation:

The distribution becomes more dispersed compared to the Caesar cipher. The original frequency peaks are partially concealed.

0.6.4 Enigma Cipher Statistics

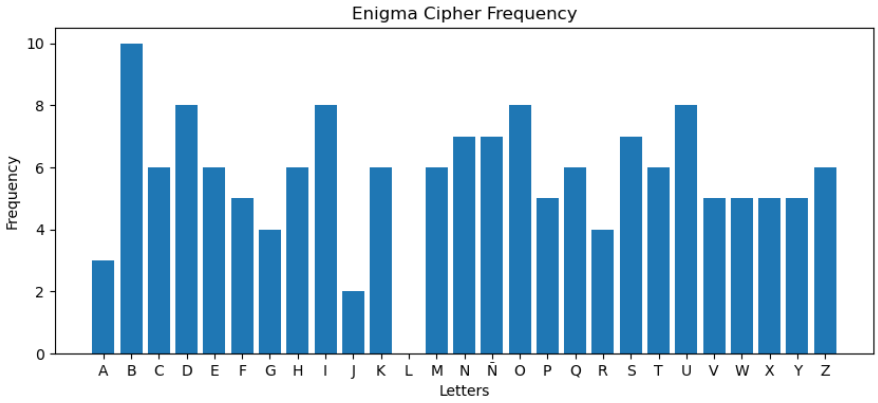

Figure 4: Letter frequency after Enigma encryption

Observation:

The distribution appears significantly more uniform. The characteristic Spanish frequency pattern is no longer easily recognizable, demonstrating stronger statistical concealment.

0.6.5 Online Enigma Simulation (Cryptii)

The following screenshot shows the encryption performed using the online Enigma simulator provided by Cryptii.

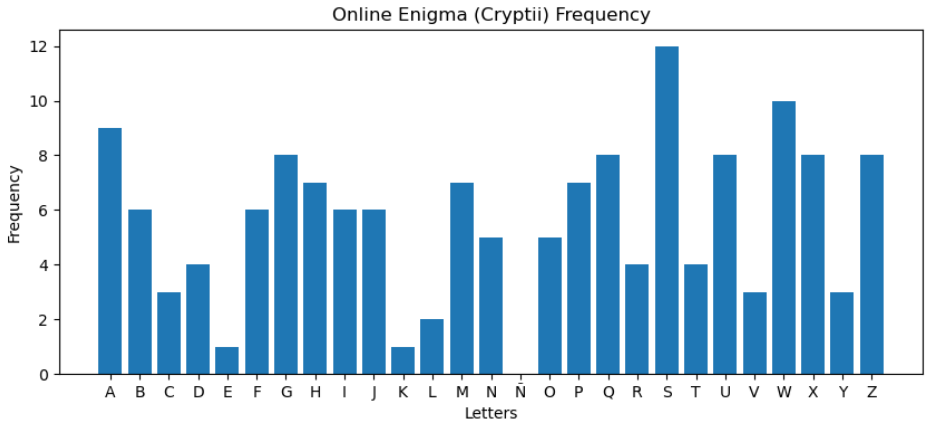

Figure 5: Online Enigma encryption using Cryptii

Observation:

The frequency distribution appears approximately uniform. The characteristic Spanish language peaks are no longer visible. This confirms that rotor-based encryption significantly reduces statistical predictability, similar to the simplified Enigma implementation.

0.7 Comparison of Statistical Properties

- The Caesar cipher preserves letter frequency structure.
- The Vigenere cipher partially hides frequency patterns.
- The Enigma machine produces a near-uniform distribution.
- Enigma encryption significantly reduces statistical predictability.

0.8 Sources Used

- Custom Python Implementation (GitHub Repository)

- Cryptii Online Enigma Simulator
- Matplotlib library for histogram generation
- Course lecture notes

0.9 Conclusion

This work demonstrates that classical substitution ciphers such as the Caesar cipher preserve the statistical properties of the underlying language. As a consequence, they remain vulnerable to frequency analysis attacks.

The Vigenere cipher improves security by applying multiple shifts based on a keyword. This reduces the visibility of clear frequency peaks, although statistical structure may still be partially detectable.

The Enigma machine introduces rotor stepping and multiple layered transformations. As a result, the ciphertext exhibits a significantly more uniform frequency distribution, making statistical attacks substantially more difficult.