Implementation and Optimization of Lattice-Based Quantum-Resistant Encryption: Advancing and Understanding Secure Cryptographic Protocols

Nathan Winningham, Department of Mathematical and Computational Sciences, The College of Wooster
Advised by Dr. John Musgrave

Project Overview

The goal of this project was to create a quantum-resistant encryption algorithm. It began with an existing scheme known as GGH-YK-M, though there was no full reference implementation—only some mathematical constraints for specific parameters. This led to the creation of a new and unique cryptosystem based on lattices and linear algebra, that combine to create a non-linear algorithm.

Data Encryption

Data encryption is broken down into two categories. The first is symmetric encryption, which uses the same key for both encryption and decryption. The other category is asymmetric encryption, which uses one key for encryption and another for decryption.

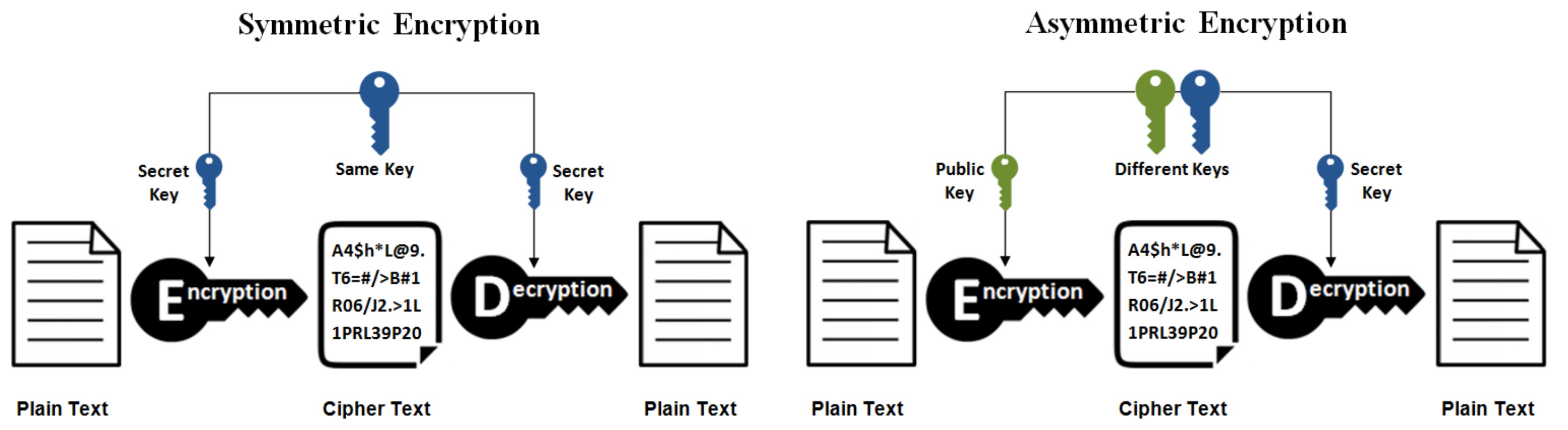


Figure 1. Encryption and Decryption Visualizations [1]

Unicode

Unicode is a numerical representation of characters—not limited to the English alphabet. It also includes special characters like newlines, characters from other languages, and even emojis. This cryptosystem converts characters from the input text file into their Unicode representations to make transformations easier to apply.

Lattices

Lattices were chosen because they leverage the use of linear algebra, which in high dimensionality are difficult to break. Algorithms such as LWE (Learning With Errors), RLWE (Ring Learning With Errors), and CVP (Closest Vector Problem) are some of the most well-known lattice-based cryptographic approaches. This cryptosystem does not follow a traditional lattice encryption method; instead, it employs high-dimensional matrix multiplication. This retains the strength of lattice-based security while introducing an additional layer of complexity—requiring more than just solving a linear matrix multiplication problem.

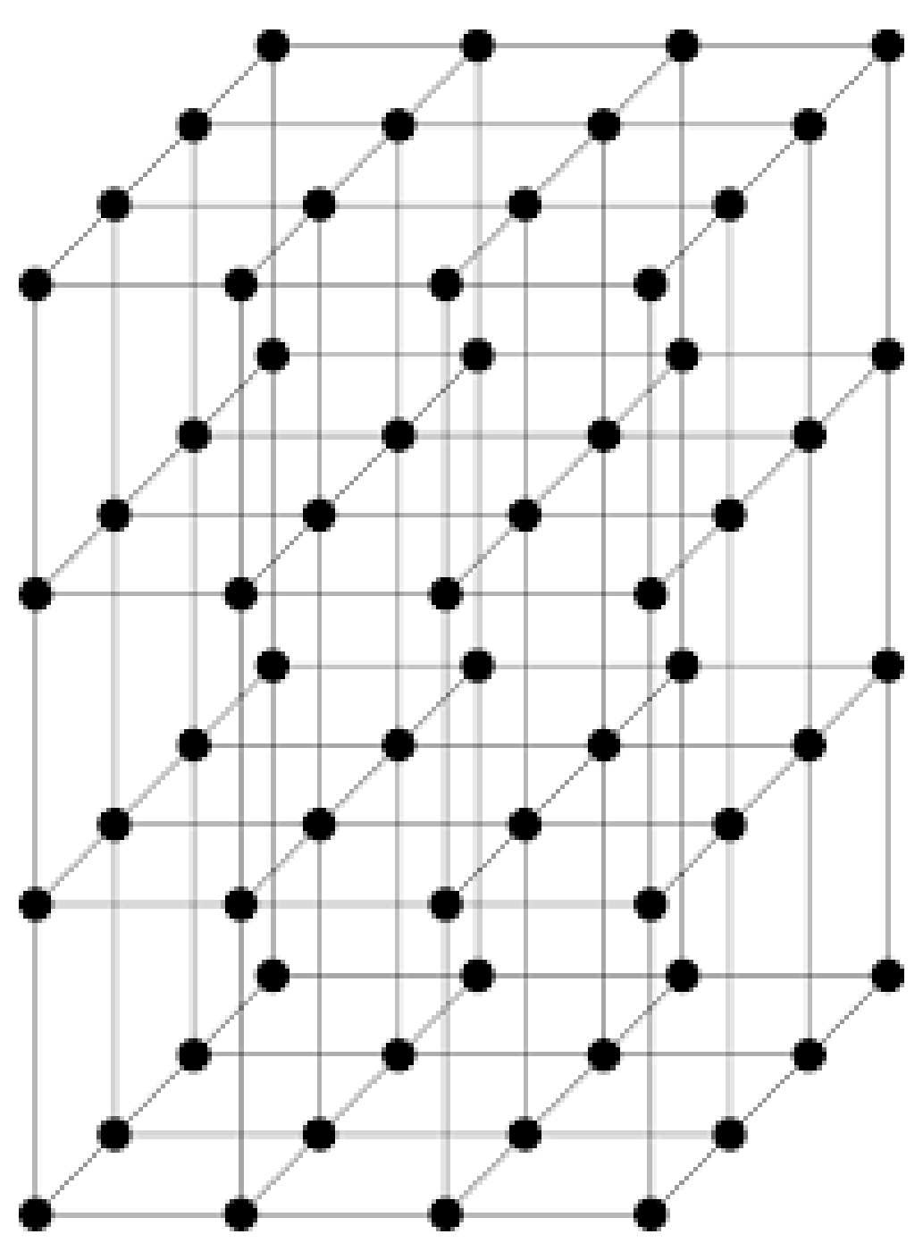


Figure 2.
Lattice Example [2]

Encryption

Encryption is broken down into five main steps:

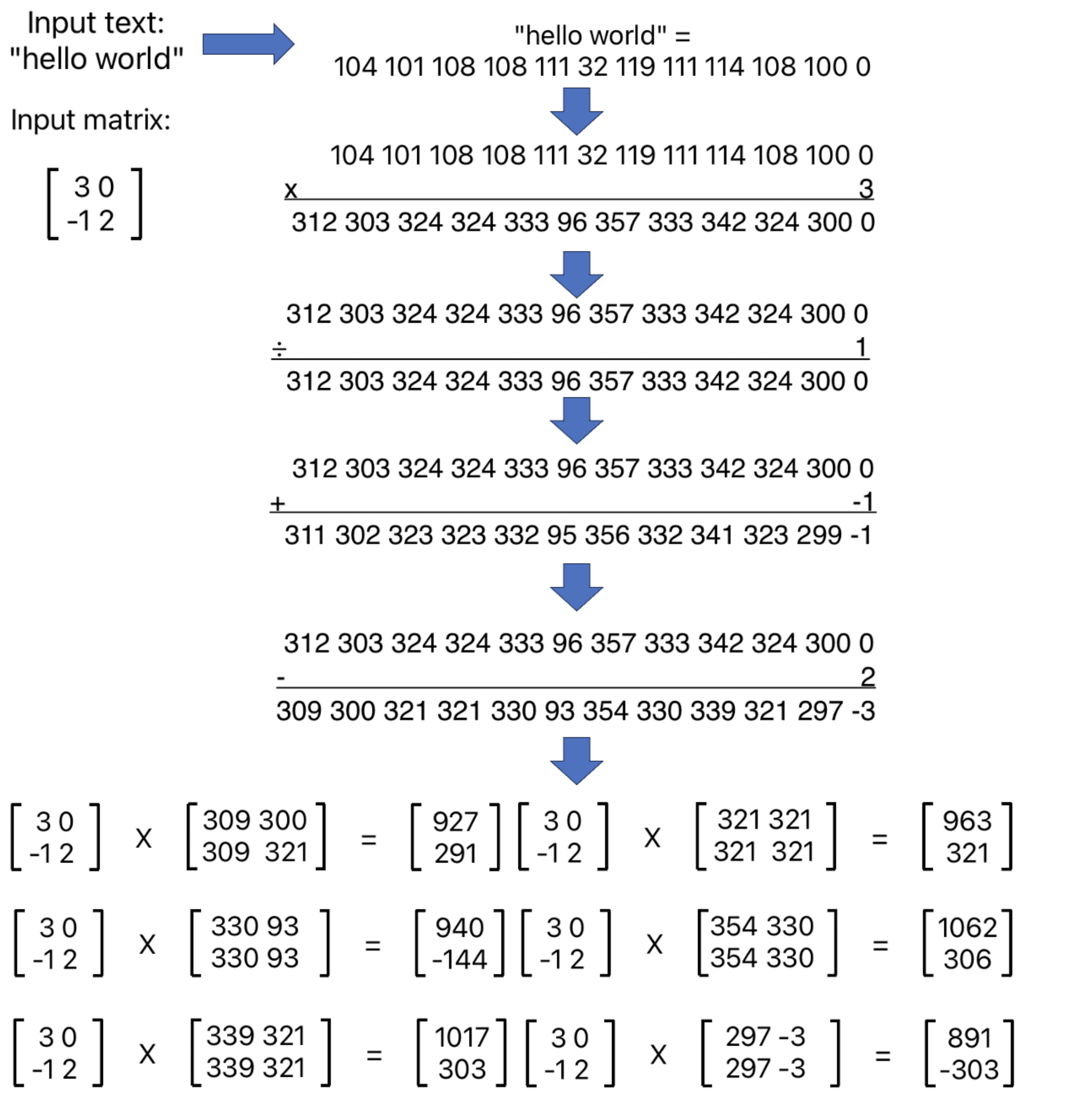
1.Input File: The user enters the pathname of the text file to be encrypted.

2.Key Generation: The user either provides or generates the m-matrix, which serves as the encryption key.

3.Scrambling: The Unicode values of the text are transformed using a series of operations—multiplication, division, addition, and subtraction—applied for as many elements as exist in the matrix.

4.Matrix Multiplication: The scrambled Unicode values are multiplied by the m-matrix using matrix multiplication. Adjustments are applied to format the resulting ciphertext properly.

5.Output: The final output includes the ciphertext, adjustment values, remainder indices, and the m-matrix (if it was generated by the system).



Input text:
"hello world"

Input matrix:

$$\begin{bmatrix}3 & 0\\ -1 & 2\end{bmatrix}$$

"hello world" =
104 101 108 108 111 32 119 111 114 108 100 0

104 101 108 108 111 32 119 111 114 108 100 0
x 3
312 303 324 324 333 96 357 333 342 324 300 0

312 303 324 324 333 96 357 333 342 324 300 0
÷ 1
312 303 324 324 333 96 357 333 342 324 300 0

312 303 324 324 333 96 357 333 342 324 300 0
+ -1
311 302 323 323 332 95 356 332 341 323 299 -1

312 303 324 324 333 96 357 333 342 324 300 0
- 2
309 300 321 321 330 93 354 330 339 321 297 -3

$$\begin{bmatrix}3 & 0\\ -1 & 2\end{bmatrix} \times \begin{bmatrix}309 & 300\\ 309 & 321\end{bmatrix} = \begin{bmatrix}927\\ 291\end{bmatrix} \quad \begin{bmatrix}3 & 0\\ -1 & 2\end{bmatrix} \times \begin{bmatrix}321 & 321\\ 321 & 321\end{bmatrix} = \begin{bmatrix}963\\ 321\end{bmatrix}$$

$$\begin{bmatrix}3 & 0\\ -1 & 2\end{bmatrix} \times \begin{bmatrix}330 & 93\\ 330 & 93\end{bmatrix} = \begin{bmatrix}940\\ -144\end{bmatrix} \quad \begin{bmatrix}3 & 0\\ -1 & 2\end{bmatrix} \times \begin{bmatrix}354 & 330\\ 354 & 330\end{bmatrix} = \begin{bmatrix}1062\\ 306\end{bmatrix}$$

$$\begin{bmatrix}3 & 0\\ -1 & 2\end{bmatrix} \times \begin{bmatrix}339 & 321\\ 339 & 321\end{bmatrix} = \begin{bmatrix}1017\\ 303\end{bmatrix} \quad \begin{bmatrix}3 & 0\\ -1 & 2\end{bmatrix} \times \begin{bmatrix}297 & -3\\ 297 & -3\end{bmatrix} = \begin{bmatrix}891\\ -303\end{bmatrix}$$

Adjustment Meanings:
Odd adjustment means the value was originally negative
Adjustment increases by 2 for each time it exceeds the Unicode Max (1114111)
Adjustments including 0.5 means that the value was a special character (0-31)
Adjustments including 0.333 means that the value was a surrogate pair character (55296-57343)

Adjustments:
0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1

(converting negatives to positives)
927 963 990 1062 1017 891 291 321 144 306 303 297 =
"OǵσŁϟЦIJCjɔj"

THE COLLEGE OF
WOOSTER

Decryption

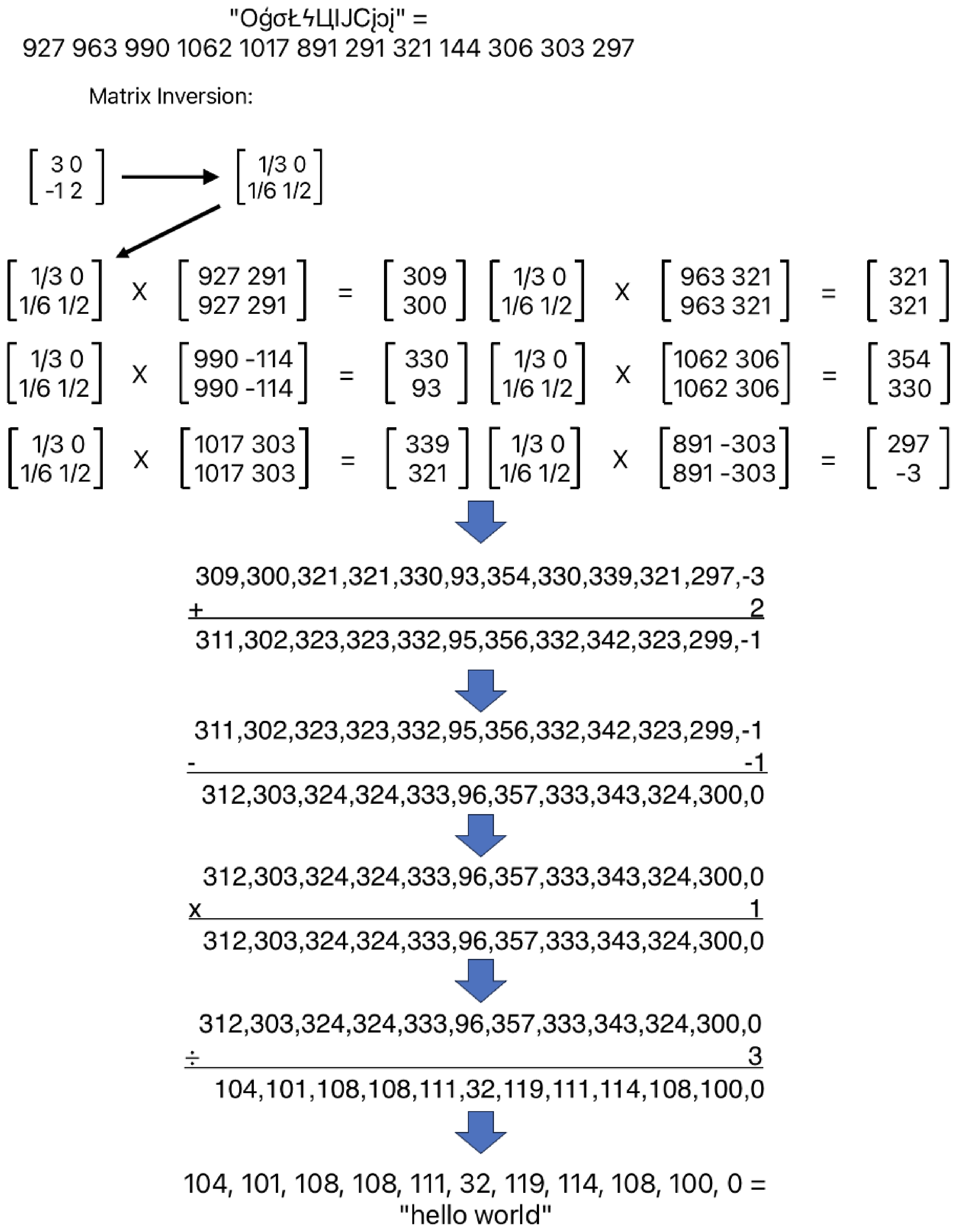
Since this cryptosystem is symmetric, decryption essentially reverts the encryption process. It consists of four main steps:

1.Input Files: The user provides the pathnames for the ciphertext, adjustments, remainder indices, and m-matrix files.

2.Matrix Inversion: The m-matrix is inverted and used to reverse the matrix multiplication, applying it to the Unicode values of the ciphertext.

3.Unscrambling: The scrambling operations are reversed and applied in reverse order—starting from the last matrix value and moving backward. This undoes the initial arithmetic transformations.

4.Plaintext Output: The final Unicode values are converted back into readable text and output as the decrypted plaintext.



"OǵσŁϟЦIJCjɔj" =
927 963 990 1062 1017 891 291 321 144 306 303 297

Matrix Inversion:

$$\begin{bmatrix}3 & 0\\ -1 & 2\end{bmatrix} \longrightarrow \begin{bmatrix}1/3 & 0\\ 1/6 & 1/2\end{bmatrix}$$

$$\begin{bmatrix}1/3 & 0\\ 1/6 & 1/2\end{bmatrix} \times \begin{bmatrix}927 & 291\\ 927 & 291\end{bmatrix} = \begin{bmatrix}309\\ 300\end{bmatrix} \quad \begin{bmatrix}1/3 & 0\\ 1/6 & 1/2\end{bmatrix} \times \begin{bmatrix}963 & 321\\ 963 & 321\end{bmatrix} = \begin{bmatrix}321\\ 321\end{bmatrix}$$

$$\begin{bmatrix}1/3 & 0\\ 1/6 & 1/2\end{bmatrix} \times \begin{bmatrix}990 & -114\\ 990 & -114\end{bmatrix} = \begin{bmatrix}330\\ 93\end{bmatrix} \quad \begin{bmatrix}1/3 & 0\\ 1/6 & 1/2\end{bmatrix} \times \begin{bmatrix}1062 & 306\\ 1062 & 306\end{bmatrix} = \begin{bmatrix}354\\ 330\end{bmatrix}$$

$$\begin{bmatrix}1/3 & 0\\ 1/6 & 1/2\end{bmatrix} \times \begin{bmatrix}1017 & 303\\ 1017 & 303\end{bmatrix} = \begin{bmatrix}339\\ 321\end{bmatrix} \quad \begin{bmatrix}1/3 & 0\\ 1/6 & 1/2\end{bmatrix} \times \begin{bmatrix}891 & -303\\ 891 & -303\end{bmatrix} = \begin{bmatrix}297\\ -3\end{bmatrix}$$

309,300,321,321,330,93,354,330,339,321,297,-3
+ 2
311,302,323,323,332,95,356,332,342,323,299,-1

311,302,323,323,332,95,356,332,342,323,299,-1
- -1
312,303,324,324,333,96,357,333,343,324,300,0

312,303,324,324,333,96,357,333,343,324,300,0
x 1
312,303,324,324,333,96,357,333,343,324,300,0

312,303,324,324,333,96,357,333,343,324,300,0
÷ 3
104,101,108,108,111,32,119,111,114,108,100,0

104, 101, 108, 108, 111, 32, 119, 114, 108, 100, 0 =
"hello world"

References

[1] Images sourced from https://www.ssl2buy.com/wiki/symmetric-vs-asymmetric-encryption-what-are-differences
[2] Image Sourced from https://tex.stackexchange.com/questions/150038/how-to-make-a-3d-lattice