

**ADVDISC**

Machine Project 1 Documentation

|  |  |
| --- | --- |
| **Section** | S19 |
| **Team Members** | Amadora, Angelo John  Andres, John Joseph  Fernandez, Ryan Austin  Syfu, Jonah Espiritu |
| **Date Submitted** | October 26, 2015 |

**Table of Contents**

I. Contribution of Each Member / 3

II. Introduction of the Research Area / 5

III. Use of Matrices and Linear Algebra Methods in the Research Area / 6

IV. Design /

V. Implementation /

VI. Conclusion /

VII. References /

**I. Contribution of Each Member**

|  |  |  |
| --- | --- | --- |
| **Member** | **Code** | **Other** |
| Andres, John Joseph |  | Quality Assurance and Testing |
| Amadora, Angelo John |  | Quality Assurance and Testing |
| Fernandez, Ryan Austin |  | Documentation  Research |
| Syfu, Jonah Espiritu |  | Quality Assurance and Testing |

**II. Introduction**

Linear Algebra is a very useful field of mathematics, especially in the field of computer science, particularly the concept of linear transformations. Linear transformations are used liberally in the field of cryptography.

Cryptography is the study of techniques in securing messages or text by enciphering them using a set algorithm. The original text is referred to as “plaintext” and the enciphered text is referred to a “ciphertext”. Decoding the ciphertext is referred to a “deciphering”. Finding the algorithm used is referred to as “cracking” or “breaking” a cipher.

The algorithm this project aims to implement is the Hill Cipher algorithm. The objective of the project is to implement the enciphering, deciphering, and the breaking of the Hill Cipher.

**III. Use of Matrices and Linear Algebra Methods in the Research Area**

**III.A. Enciphering Using the Hill Cipher**

A Hill-n Cipher makes use of an nxn matrix A and a modulus n. The only requirements of the matrix are that its determinant have a modular inverse with respect to the modulus. This means it does not have any common prime factors.

Once an appropriate matrix is found, a plaintext string is enciphered by first transforming it into a matrix. This is done by first representing the string as its numerical representation.

Assume the scheme is the number’s cardinality in the English Alphabet. Take the string BEATRICE. Our modulus is therefore 27 since the values 0 – 26 are being used, 0 representing a whitespace. This would be represented as

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| B | E | A | T | R | I | C | E |
| 2 | 5 | 1 | 20 | 18 | 9 | 3 | 5 |

This is then transformed into vectors in Rn depending on the cipher parameters. Assume a Hill-3 Cipher is being used. The word is transformed into 3-tuple vectors. Any missing characters are pumped with a space.

Let the matrix A be whose determinant is -10, which has no common prime factors with 27 and is thus a valid matrix.

To encipher the message, the vectors created from the message are collated into a single matrix X. The ciphertext comes from the product Y = AX mod 27, where the column vectors of Y are the corresponding vectors of the ciphertext.

Which translates to

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 21 | 17 | 14 | 4 | 1 | 20 | 21 | 20 | 13 |
| U | Q | N | D | A | T | U | T | M |

So the corresponding ciphertext for BEATRICE in this cipher scheme is UQNDATUTM.

**III.B. Deciphering**

To decipher the ciphertext, first we must get the inverse of the enciphering matrix A. This is done slightly differently than the regular method. First, the adjunct of the matrix is computed. This is simply the transpose of the matrix containing all the matrix’s cofactors.

For the matrix above, the adjunct is

Normally, the inverse is found by multiplying the adjunct by the multiplicative inverse of the determinant, but inverse is now computed by multiplying the adjunct with the multiplicative modular inverse of the determinant. The multiplicative modular inverse of a number modulo m is a number a-1 such that aa-1 = 1 mod m.

The determinant of the original matrix was -10. The multiplicative modular inverse is then 8 since -10(8) = 80 = 1 mod 27.

The inverse is then

So taking the ciphertext UQNDATUTM, translating into

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| U | Q | N | D | A | T | U | T | M |
| 21 | 17 | 14 | 4 | 1 | 20 | 21 | 20 | 13 |

Which is converted into the matrix .

The plaintext is gotten by multiplying A-1Y mod 27.

Which translates to

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 2 | 5 | 1 | 20 | 18 | 9 | 3 | 5 |
| B | E | A | T | R | I | C | E |

Which is the original string from the previous chapter.

**III.C. Breaking the Cipher**

Given a plaintext “BEATRICE “ and a ciphertext “UQNDATUTM”, the original enciphering matrix could be derived.

Let p1, p2, …, pn be linearly independent plaintext vectors and c1, c2, …, cn be the corresponding ciphertext vectors, the deciphering matrix could be derived by forming first matrices C and P, C having c1T, c2T, …, cnT as row vectors and P having p1T, p2T, …, pnT as row vectors, augmenting P to C, forming [C|P] and row reducing that matrix to [In|(A-1)T]. A-1 is the transpose of the right half of the augmented matrix.

So using the same example, are linearly independent plaintext vectors and are the corresponding ciphertext vectors.

[C|P] is then formed by

Row reducing…

**IV. Design**

**V. Implementation**

The Java programming language was used, where Java Swing was used for the Graphical User interface.

**VI. Conclusion**

**VII. References**

Anton, H. & Rorres, C. (2010). *Elementary linear algebra: Applications version*. John Wiley & Sons, NJ:

New Jersey.

Cryptography. (n.d.). Retrieved November 5, 2015, In Wikipedia: https://en.wikipedia.org/wiki

/Cryptography