Core Mathematics Coursework

Applications of Matrices in Cryptography

Matrices are a part of everyday life and culture. It can be applied in real life as a form of calculation and/or collection of data, much like statistics, but much more restrained and harder to understand when one sets his eyes upon it. However, they are essential n certain applications, notably in the secure encryption and decryption of data.

Matrices are numbers that are arranged rectangular in a big bracket, arranged in rows and columns. An example of a matrix would be this: As it can be seen, the numbers are arranged as such in a matrix. A use of matrix in everyday would be the collection of data from: a store, or even a school.



Lets say that at certain schools, the population of a cohort has been compiled into a table as shown:

|  |  |  |  |
| --- | --- | --- | --- |
| **Gender** | **Dunman Secondary School** | **Jurong Secondary School** | **River Valley High School** |
| **boys** | 230 | 250 | 225 |
| **girls** | 223 | 229 | 249 |

In this report, we will be investigating the use of matrices and vectors in cryptology. We collectively decided to focus on this because we were interested in their use in the military.

Our aim is to examine the use of matrices in encryption, and it's uses in a specific encryption called the Hill Cipher. Other types of math can applied here, such as vectors. We will also briefly summarize and explain the uses of modular arithmetic or 'clock math' in the Hill Cipher, which is essential to the understanding of the cipher. Once we do this, we will attempt to decrypt the Hill Cipher.

The following report assumes an elementary understanding of matrices.

**ENCRYPTION**

To encrypt a message, first you need to find a message to send. This unencrypted message is called the plaintext. Let’s take the sample message, “HELLOWORLD”. We must first encode it into a matrix using an alpha-numeric conversion process

For reasons that will be discussed later, we use a base of 29 to reduce our matrix, that is, we will use 29 characters in our alphabet.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| \_ | A | B | C | D | E | F | G | H | I | J | K | L | M |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| N | O | P | Q | R | S | T | U | V | W | X | Y | Z | , | . |
| 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 |

Here, our plaintext converts into (8 5 12 12 15 23 15 18 12 4)

Then, we create a key, which is the matrix that we will use to encode our matrix. Let our key be “PONY”. Since our key is 2 by 2, we can represent it as



However, since our message matrix is unable to multiply with the 10 by 1 matrix, we will alter it to fit, by making it a 5 by 2 matrix.



Now, using our Graphic Display Calculator (GDC), we will multiply the both of them together.

 =



Matrices are an excellent way to scramble data because of the jumbling effect of multiplying matrices. The following matrix is almost unrecognizable from its original code. However, it is often impractical to send matrices, as it arouses suspicion. So what can we do to change the converted matrix to alphanumeric characters? The answer: Modular arithmetic.

Modular arithmetic, also known as ‘clock math’, is a number system whereby numbers cannot exceed a certain value, but instead ‘overflow’ and become 0. For example, 22 7 (mod 15). Even large numbers will reduce to regular numbers if we use clock arithmetic. In other words, large numbers can be reduced to their congruent basic forms by finding the remainder when divided by the base.



|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| \_ | A | B | C | D | E | F | G | H | I | J | K | L | M | N |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| O | P | Q | R | S | T | U | V | W | X | Y | Z | , | . |
| 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 |

Normally, modular arithmetic is a laborious process to do by hand, by finding the remainder of each number. However, it is easy to do with the GDC! The “Remainder” function is extremely useful for this.

For example, to find the reduced value of 342 in mod 42, we simply enter

remain(342,42) = 6

And doing the same with a matrix is equally easy!

= 

So, we get a plaintext of “IO,XJTJIDT”, which we can send to the recipient, at which point, decryption can begin.

**DECRYPTION**

After receiving the message, recipient finds the inverse of the pre-agreed key’s matrix.

However, what happens when the determinant of our key is 0? Take for example our sample key “MEME”



= NA

As you can see, when the determinant is 0, the matrix cannot be used. This is because the matrix does not have an inverse, so when the recipient tries to decrypt the encrypted matrix, one is unable to do so.

Thus, “PONY” is better than “MEME”.

We also run into problems if the determinant of the matrix has common factors with the base of our alphanumeric system. However, this can be solved by using prime numbers as our base, which is why we are using an alpha-numeric conversion with 29 characters.

Finding the modular inverse of matrices is largely the same as normal matrix inverses, but with one notable exception.

= 190-1

Modular inverses work thus; an integer multiplied by it’s modular inverse is 1.

190-1(20) = 1 (mod 29)

Thus,

20=   (mod 29)



We can confirm that this is indeed the inverse matrix by multiplying them together and looking for the identity matrix.

 =  (mod 29)



Let us begin the process of reversing the encryption, by turning the encrypted message back to matrix form and multiplying the matrix by the inverse of the key matrix.



And then reducing the matrix to its basic form:

= (mod 29)

And converted back to text, is, HELLOWORLD, which was our encrypted message!

**CONCLUSION**

In conclusion, matrices can be used to code hidden and secret message, as it can be seen by the hill cipher. Also, matrices can be used in other ways in our way of life, and this is a very good way of compiling and collecting data, not to mention have fun in terms of coding.

The Hill Cipher might be weak and that people might get a hold of the information you are sending secretly but when it is combined with other types of ciphers such as public key, it is very effective in staying secret and unexploited to the point where no one will find out your secret information, and that only the person who you are sending it to will understand the message.

However, one limitation is that without the help of a GDC or encrypting device, it will be very hard for someone to decode the message and that if the person wishes to decode the message by hand will have a hard time as he would have to mentally calculate all the matrix equations. With the help of a GDC, one can finish the decoding and coding sequence quickly, reducing time taken and getting the message across faster.

It all depends on whom you’re trying to hide from. If you’re trying to hide from your parents’ prying eyes or your peeking little brother, a simple letter substitution or other simple cipher will suffice. If you’re trying to transmit data without competitors finding your top-secret product, perhaps a more advanced cipher will have to be used.