Application of Linear Algebra in Cryptography

M. Thiruchelvi

Abstract--- *Information is a message which is received and understood. Information can be sent one person to another over a long range but the process of sending information must be done in a secure way especially in case of a private message. Mathematicians and Engineers have historically relied on different algorithmic techniques to secure messages and signals. One field in linear algebra's broad range of applications is Cryptography, the study of securely transmitting data over insecure channels. Instances of basic cryptography are evident throughout recorded history, seen in Da Vinci's notebooks, and used heavily for secure communications in war. As long as people have been able to write, there has been a need for communicating sensitive information. With advances in mathematic operations and computing power, the need, and also capability, of cryptography is constantly increasing. Today, Cryptography plays an important part in online services such as bank transactions, online currencies, and all sorts of services where secure transmission is necessary. In this paper, I present fundamentals of the field of cryptography that rely heavily on tools defined by linear algebra.*

I. Introduction

ENCODING is the transformation of data into some unreadable form. Its purpose is to ensure privacy by keeping the information hidden from anyone for whom it is not intended. Decoding is the reverse of encoding; it is the transformation of encrypted data back into some intelligible form. Cryptography is popularly known as the study of encoding and decoding private messages. Because its importance, there is a recent surge of interest in cryptography.

II. Caesar Cipher

Until recently, encrypting secret messages was performed by hand using relatively trivial mechanisms to disguise information. One of the most well-known ciphers was named after Julius Caesar, namely, the Caesar cipher. The Caesar cipher is an example of a substitution cipher. Each letter of a given plaintext, the information to be encrypted, is substituted with another letter some given number of positions from it in the alphabet. For example, if we had an alphabet comprised of the standard 26 letters in the English alphabet and swapped each letter with the letter three places after it in the alphabet; we would have the following Caesar cipher.

M. Thiruchelvi, Head, Department of Mathematics, Sankara College of Science and Commerce, Saravanampatti, Coimbatore – 641 035. E-mail: m.thiruchelvi@gmail.com

- *Cipher text:*

Using this cipher, the text "TOP SECRET MESSAGE" would encode to "WRS VHFUHW PHVVDJH." One of the main problems with the Caesar cipher is that if an individual intercepts the cipher text and guesses that the Caesar cipher was used for the encryption, he or she could easily go through the 25 shift values until they come upon a shift that decodes the cipher text into a meaningful plaintext. For example, if a substitution cipher encoded "e" to "h," "h" would occur in the cipher text with the same frequency as "e" in the original language, allowing for a relatively simple analysis to break the substitution cipher

- *Hill Cipher:*

As time progressed, the study of cryptography continued to mature and, more recently, began to involve higher level mathematics. With this more advanced math came more advanced ciphers based on the idea of encryption and decryption keys. Encryption keys are a special value or set of values used in an encryption algorithm to convert a plaintext into a cipher text. A decryption key is the opposite. Decryption keys are used as part of a decryption algorithm to convert the cipher text back into the original plaintext. One such example of an encryption scheme that utilizes more advanced mathematics, as well as encryption and decryption keys is a cipher from 1929 called the Hill cipher. The Hill cipher is based on linear algebra and overcomes the frequency distribution problem of the Caesar cipher that was previously discussed.

To illustrate some of the foundations of cryptography, say person A wanted to send person B a private message of the text, "TEST MESSAGE". This unencrypted message is called the plaintext. A logical first step to encrypting plaintext is to assign and replace every possible character in the message with an integer value. Since computers only fundamentally deal with numbers, a map from a character to an integer value makes it easier for the computer to algebraically manipulate each character. This map is usually called a substitution cipher. By this simple example, hope to understand this technique of encryption, known as the Hill cipher, is one of the most elegant ways to illustrate the roots of all cryptography in terms of linear algebra, as well as an excellent way to illustrate an application of matrix algebra and other properties. Hill cipher is insecure since it uses linear matrix operations. An attacker knowing a plaintext and ciphertext pair can easily figure out the key matrix.

- *Block Ciphers*

Plaintext is divided into blocks of fixed length and every block is encrypted one at a time.

A block cipher is a set of 'code books' and every key produce a different code book. The encryption of a plaintext

ISBN 978-93-83459-16-2 © 2014 Bonfring

block is the corresponding ciphertext block entry in the code book. There are several methods to encrypt *M*, which is referred to as *block-cipher modes* of operations. Standard block-cipher modes of operations:

- *Electronic Code Book mode (ECB)*
- *Cipher Block Chaining mode (CBC)*

- *Electronic Code Book Mode (ECB)*

There are innumerable methods of increasing the security of an encryption algorithm. The method of encoding that the basic Hill cipher uses, such that each unique plaintext input corresponds to a unique ciphertext output, and each input is encrypted independently from all others, is known as the Electronic Code Book (ECB) method. Let C_i be the *i*-th ciphertext block: ECB is often used to encrypt short plaintext messages. However, if we break up our string into blocks, there could be a chance that two blocks are identical: $M_i = M_j$ ($i \neq j$). This provides the attacker with some information about the encryption.

Enacting the example cipher from above string "EASYTOBREAK" results in the ciphertext "XYXSCYVTXYAD" including the calculated appended character, while the slightly modified string "EASYTOCREAK" results in the ciphertext "XYXSCYKXXYBI".

- *Cipher Block Chaining (CBC)*

A way to increase the difficulty of breaking a cipher is to use Cipher Block Chaining (CBC) as a method of encryption instead of ECB. Instead of having a direct map to from plaintext to ciphertext as in the ECB, CBC saves the ciphertext value of previous encryptions, and enacts a function involving that value on the plaintext before encrypting it with the main cipher. This method increases security in two ways. Using this method adds a level of abstraction to the encryption process, making it harder to crack the cipher, as well as introduces a method of validation for all messages. To illustrate CBC, I will extend the Hill cipher example used previously. The way a computer fundamentally deals with numbers is in binary notation, meaning each digit is either a 0 or a 1. For a CBC, the function often used between the previous ciphertext and the current plaintext is a bitwise XOR. A bitwise XOR iterates through binary strings, comparing each significant digit, and returning 1 if there are an odd number of 1's between the two, and 0 otherwise.

Say I want to encrypt the plaintext string "ALWAYSBETTER", referred to as p1, using the ciphertext string "XYXSCYVTXYAD" from earlier, referred to as c0, as the block. Next, I convert p1 to its integer form, which is "1 12 23 1 25 19 2 5 20 20 5 18", and recall the integer form of c0, which is "24 25 24 29 3 25 22 20 24 25 1 4".

For this cipher, the largest integer value we need to represent in binary is 26. Recall that each binary digit represents a power of 2. Representing a decimal number n in binary involves a linear combination of m powers of 2, where $n < 2^m$. Solve this relation for m and add a ceiling operator to establish the following equation for determining m, the number of bits needed to encode a set of n values.

$$m = \lfloor log_2 m \rfloor$$

Using this equation, it is clear that only need 5 bits to represent 1-26 in binary. Determining each number's representation is a simple greedy algorithm, which subtracts each power of 2 from the desired number. If the subtraction is greater than or equal to 0, then perform it and set that bit equal to 1. Otherwise, do not perform the subtraction and set that bit equal to 0. Calculate and compare each significant digit of c0 and p1.

c0 = 11000 11001 11000 10011 00011 11001 10110 10100 11000 11001 00001 00100

XOR

p1 = 00001 01100 10111 00001 11001 10011 00010 00101 10100 10100 00101 10011

The result of this calculation will be referred to as p1' and is shown below

p1'= 11001 10101 01111 10010 11010 01010 10100 10001 01100 01101 00100 10111

Now convert this binary string to back to decimal and get the integer string "25 21 15 18 26 10 20 17 12 13 4 23". Then, assemble a 3×4 plaintext matrix and multiply it by the key matrix.

$$c1 = k.\ p1 = \begin{bmatrix} 3 & 3 & 4 \\ 0 & 1 & 1 \\ 4 & 3 & 4 \end{bmatrix} \begin{bmatrix} 25 & 18 & 20 & 13 \\ 21 & 26 & 17 & 4 \\ 15 & 10 & 12 & 23 \end{bmatrix} =$$

$$\begin{bmatrix} 198 & 172 & 159 & 143 \\ 36 & 36 & 29 & 27 \\ 223 & 190 & 179 & 156 \end{bmatrix}$$

This sort of transformation seems as though it would be one way, and an inverse function to decrypt the text could not be found. However, the bitwise XOR function is actually its own inverse, meaning applying the function to a string twice will return the original string. The recipient first applies the inverse matrix key to the ciphertext c1 to get p1' back.

$$p1' = k^{-1}.c1 = \begin{bmatrix} -1 & 0 & 1 \\ -4 & 4 & 3 \\ 4 & -3 & -3 \end{bmatrix}$$

$$\begin{bmatrix} 198 & 172 & 159 & 143 \\ 36 & 36 & 29 & 27 \\ 223 & 190 & 179 & 156 \end{bmatrix} = \begin{bmatrix} 25 & 18 & 20 & 13 \\ 21 & 26 & 17 & 4 \\ 15 & 10 & 12 & 23 \end{bmatrix}$$

We then perform a bitwise XOR on c0 and p1'

c0 = 11000 11001 11000 10011 00011 11001 10110 10100 11000 11001 00001 00100

XOR

p1'= 11001 10101 01111 10010 11010 01010 10100 10001 01100 01101 00100 10111

and get back

p1 = 00001 01100 10111 00001 11001 10011 00010 00101 10100 10100 00101 10011

ISBN 978-93-83459-16-2 © 2014 Bonfring

This is the exact bit string that was sent earlier! Which is “1 12 23 1 25 19 2 5 20 20 5 18”, Since the ciphertext string c0 is transmitted publicly over the insecure channel, every intended recipient knows the value they need to use for the bitwise operation. While only a marginal increase in security, CBC allows an encrypted storage of message history, which is computationally infeasible to edit.

III. Conclusion

If two people who wish to communicate have access to a secure channel over which they can share the key, then this is easy to do, but ultimately, they could just share their message over that channel. Also, in today’s age of global communication, there is almost no such thing as a secure channel. A major issue in cryptography is how to share a key over an insecure channel. An encompassing term for the method most commonly used to deal with this issue is public-key cryptography, in which every user has access to the key, which encrypts the data. Typically, this key is a special function in which it is very easy to calculate one way, making it trivial to encrypt items, but is computationally impossible to calculate the inverse function, and instead, each user keeps a separate function to decrypt data private and secure. To know more about these functions, search for public-key cryptography, particularly the RSA algorithm and the Diffie-Hellman key exchange protocol. While matrix-based ciphers are not the most secure form of encryption, they are useful for illustrating the fundamental concepts of the field of cryptography, and are a common choice to do so.

References

[1] J.-S. Coron. “What is Cryptography?” *IEEE Security & Privacy,* vol. 4, no. 1, 2006, pp. 70-73.

[2] M. Mokhtari and H. Naraghi. “Analysis and Design of Affine and Hill Cipher,” *Journal of Mathematics Research,* vol. 4, no. 1, 2012, pp. 67-77.

[3] A. McAndrew. “Using the Hill cipher to teach cryptographic principles,” *International Journal of Mathematical Education in Science & Technology,* vol 38. No. 7, 2008, pp. 967-979.

[4] W. Diffie and M. E. Hellman. “New Directions in Cryptography,” *IEEE Transactions on Information Theory,* vol. 22, no. 6, 1976, pp. 644-654.

ISBN 978-93-83459-16-2 © 2014 Bonfring