International Journal of Electronics Communication and Computer Engineering
Volume 6, Issue 3, ISSN (Online): 2249–071X, ISSN (Print): 2278–4209

Mathematical Model for Classical Cryptography

Dr. Mahdi F. Mosa
(M.Sc. Liverpool, PhD Bradford), Engineering Mathematics,
AMA International University Bahrain
Email: madimosa@yahoo.com

***Abstract* – In this article we present a mathematical model for classical encryption of a plain text for secure confidential information through unsecure channel. The method of encryption based on the generation of prime numbers, seventh order number system and mathematical theory of matrices. We form the matrix A for the plain text, for simplicity of calculation. The result shows that this model provides an acceptable secure exchange of information within a close circle net of a company and it can be on wider than that. The 7 system is a system with seven numbers namely (0,1,2,3,4,5,6) with radix 7 and we can change any decimal number or other system number to the 7 system. The receiver has the password and the process of encryption to decrypt the message. Also we notice that this model can be wider through bilingual and other system of numbers.**

***Keywords* – Cryptography, Prime Numbers, Seventh number System and Theory of Matrices with Example.**

I. INTRODUCTION

The growth of, business and information in general, electronic communication through internet activities are the most important in the world of today and in that the security factor keeping the people in companies, large or small, private or general, in a continues concern from hacking. In this sense most companies need a private security system to save their information from hackers.

Security of information through any form of internet means hiding the information from spies and may be other form of discrepancy, by some algorithm that transform the clear text (plaintext) to other form of information, which is called encryption [8].

The encryption methods in both cases the classical and modern are process through algorithms [4, 7]. In this article the encryption process takes place by linear algebra especially matrix theory [8], section (1) and a usage of a prime numbers generated by some function with the seventh system numbers [3], section (2). That is, the final output of these activities has been encrypted by two methods, section (3). At the end the results and conclusion will be given with a list of the reference. The history of encryption is as old as the creation of the international human at this plant, but what I saw in some references for the last four thousand year some text were found encrypted at the Veterans Egyptian where the hieroglyphic inscriptions on the tomb of the nobleman khnumhotep II [6]. Later about 2000 years ago, the Greek knew cylinder device called Scytale was used and it similar to transposition technique [5]. Around 1200 year ago Sheikh Al-Kindi in his book "Risalah fi Istikhraj Al-Mu,am (Manuscript for Deciphering Cryptographic Messages) used a frequency analysis technique for breaking monoalphabetic substitution ciphers which was in use, until world war two [2]. Then, the development of the polyalphabetic cipher by Leon Battista Albert, who is known as the father of western cryptology, in 1465 [6, 9]. After that the subject of cryptography start growing fast, Trithemius(1518), Vigenere (1585), Wheatstone and Playfair(1854), Kerkhoff (1833), Hill(1929) and until the time of Diffie –Hellman (1976). In all the mentioned researchers above are presented methods of classical cryptography including mathematical models in matrix algebra, but however we noticed that there is no article including a combination of prime numbers and the seventh number system including the manipulation presented by Hill [1].

This article shows aneasy and effective way for encryption process in a sequence of mathematical operations and the criteria which will be given in the other sections of this paper, can summarized by the following steps :

1- Language English and it can be in any other language or double or more languages. The 26 alphabets of English are:

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

2- We take a 26 prime numbers, some of them are generated by the algebraic equation $y = n^2-n+41$, such that 1,3,5,7,11,13,17, 19, 23,29,31,37, 41,43, 47, 53, 61 , 67, 71, 83,97,113,131, 151, 173,197, or more and we can chose, for our purpose, any other prime numbers. It can be noted for example that the numbers 1,3,5,7,11,13, 17,19,23,29,31,37 are prime numbers not generated by the above function but it is a choice of the author.

3- Assign each alphabet to prime number of the language in sequence.

Table 1: Assign each alphabet to prime number of the language in sequence (part 1).

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q
1	3	5	7	11	13	17	19	23	29	31	37	41	43	47	53	61

Table 1: Assign each alphabet to prime number of the language in sequence (part 2).

r	s	t	u	v	w	x	y	z
67	71	83	97	113	131	151	173	197

International Journal of Electronics Communication and Computer Engineering
Volume 6, Issue 3, ISSN (Online): 2249–071X, ISSN (Print): 2278–4209

4- Take any plain text, for example AMAIUBAHRAIN.
5- Encrypt the text using the prime numbers as in table (1).

Table 3: Encrypt the text using the prime numbers.

a	m	a	i	u	b	a	h	r	a	i	n
1	41	1	23	97	3	1	19	67	1	37	43

6- Form a square matrix, say A, (or more than one matrix), with the prime numbers are the elements as in table (2). In this case we have to use a square matrix A with 4 column and 4 rows which means we have to add 4 vague elements in the end of matrix, such that, Table 3.

Table (3): Vague elements in the end of matrix.

$$A=\begin{bmatrix}1 & 41 & 1 & 23\\ 97 & 3 & 1 & 19\\ 67 & 1 & 37 & 43\\ 3 & 5 & 3 & 5\end{bmatrix}$$

Where 3=b & 5=c are vague quantities.

7- Form a new matrix, B≠0 , similar in size to the matrix A, with any elements, which represent the pass-word. In this case we can always split a large square matrix to small square matrices and

8- A new matrix C= AB is formed.

9- The system of numbers in everyday use is the denary or decimal system of numbers, using the digits 0 to 9. It has ten different digits operation on the matrix C, we change all the elements to any other number system and we chose the seventh number system, which has seven different digits (0, 1, 2,3,4,5 and 6) and a radix of 7.The denary number equivalent to the 7th system number (493)10 =(1303)7 , (11)7 =(8)10 and (52)7= (37)10 and so on.

10- After the change of elements of C to the new form in 9 above and for the purpose of hiding the used number system we add the number 33 or any other number to each element of the matrix and then send to the receiver in the other side.

11- Decryptions:

a- Subtract the number 33 from each element of the encrypted matrix.

b- Change the elements to the denary system.

c- $A = B^{-1} C$.

d- Use the standard table for the encryption process, to have the plain text.

This paper usually important in applications in most of the discipline of the life specially the cases of companies of industries when they seems to be sensitive to the problem of security concerns from attack through the transfer of information through unsecure channels, so the needs of cryptography is needed.

This research shows an easy and effective way for encryption process in a sequence of mathematical operations and the criteria.

II. Research Methodology

As we mentioned above about the encryption process can be in any language. We form the matrix A for the plain text, for simplicity of calculation, let as take lani, using the English alphabets, such that

$A=\begin{bmatrix}43 & 53\\ 71 & 83\end{bmatrix}$ and a password $B=\begin{bmatrix}3 & 7\\ 11 & 13\end{bmatrix}$ then a new matrix C can be formed such that $C=AB=\begin{bmatrix}712 & 990\\ 1126 & 1576\end{bmatrix}$.

Usually, one can stop to this level but for more security, the seventh numbers system is used on the elements of matrix C, then C becomes:

$C=\begin{bmatrix}2035 & 2613\\ 3166 & 4411\end{bmatrix}$ and add to each element the number 33, the matrix C becomes:

$C=\begin{bmatrix}2068 & 2646\\ 3199 & 4444\end{bmatrix}$,

Send 2068 2646 3199 4444.

In this place we can mention some useful notes:

1- The 33 decimal number (or any other decimal number) is added in the end of the encryption process to each element of the final matrix C to deviate or hide the used number system for the seek of more security.

2- The size of the matrix B is the same as the matrix A and it satisfies the rules of matrices multiplication (the number of columns in the first equal to the number of rows in the second matrix) and I choose square matrices A and B of the same size, for further security of the password of the system. It must be clear to the reader that a square matrix of any size always can be split to many small square matrices with the same password. For example take the plaintext AMAIUB Bahrain, these are display in table (2) such that:

$A1=\begin{bmatrix}1 & 41\\ 1 & 23\end{bmatrix}, A2=\begin{bmatrix}97 & 3\\ 1 & 19\end{bmatrix}, A3=\begin{bmatrix}67 & 1\\ 37 & 43\end{bmatrix}$.

Then there are three matrices of the same size and we can introduce a password

$B=\begin{bmatrix}5 & 11\\ 23 & 7\end{bmatrix}$

which can be multiply by each matrix A1, A2 and A3. This means that any message of any size can be written as small square matrices.

Decryption:

The other party have to use his knowledge about the process (prime numbers, alteration of numbers of some characters and the seventh numbers system) in addition to the password, such that : Subtract 33 from each element in the matrix, then change the received seventh system numbers to decimal numbers system, $2035_7=712_{10}$, $2613_7=990_{10}$, $3166_7= 1126_{10}$, $4411_7= 1576_{10}$. In the usual elementary way of matrices operation we can find the inverse of the matrix A.

From algebra $AA^{-1}= I$, where A^{-1} is the inverse of the matrix A and I is the unit matrix. Then $C = AB$ leads to $A = CB^{-1}$ and

$B^{-1}=\begin{bmatrix}-13/38 & 7/38\\ 11/38 & -3/38\end{bmatrix}$, thus $A=\begin{bmatrix}43 & 53\\ 71 & 83\end{bmatrix}$= lani.

III. Results and Discussion

In this article a mathematical model was presented through a prime numbers system and the seventh number system with a radix of 7. Algebraic theories of matrices have been used and an applied example is given. The results of encryption and decryption showed that this

model seems to be quite reasonable, for a company security system. This model can be modified in many ways such as the usage of double languages and other number system with a prime number system. It must be noted that no system of encryption has an absolute security with a hackers continues attack but it is needed in these days technology to increase a possible security of exchange of information. 3. There is no division 33. This number is added in the end of the encryption process to hide the used number system for the seek of more security (as mentioned in the article we can take number to add to each element. The 7 system is a system with seven numbers namely (0,1,2,3,4,5,6) with radix 7 and we can change any decimal number or other system number to the 7 system. The Receiver has the password and the process of encryption to decrypt the message.

In comparison with other works of the references of this article we showed that the function: $F(n)=n^2-n+41$, can generate some prime numbers with an additional security through the seventh numbers system plus any decimal integer to hide the used number system, which are produce a reasonable security system for the information of a company exchange of information.

The computational time of such a system is usually quite limited because there are no complicated operations required.

IV. Conclusion

The final finding of this article is:

1- Mathematical tools are always leaded to solutions for the obstacles in society.

2- The prime numbers system and non-classical number system with matrices lead to reasonable security and may be sufficient for a close loop for a company information system.

3- This model can be organized in a computer program using, c++ for example, or a data base system.

References

[1] Lester S. Hill, (1929). Hill Cipher- Wikipedia, the Free Encyclopedia.

[2] Badeau, J. (1983). "The genius of the Arab civilization", Second Edition.MIT Press, USA.

[3] Alireza N. Pour, (2002). Number Theory and Related Algorithms in Cryptography, Master of Information Science Thesis, Japan Advanced Institute, Japan.

[4] Cameron, P. J. (2003). School of Mathematical Sciences, Queen Mary, University of London, Notes on Cryptography, England.

[5] Dieter, G. (2005), Computer Security, Second Edition, John Wiley and sons, UK.

[6] Forouzan, A. (2007). Cryptography and Network Security, First Edition, McGraw-Hill, USA.

[7] Delfs, H.andKenbel, H. (2007). Introduction to Cryptography, Second Edition, Springer- Verlag Berlin Heidelberg.

[8] Jeffrey Hoffstein, Jill Pipher, Silverman, J.H. (2008). An Introduction to Mathematical Cryptography, First edition, Springer Science and Business Media, Germany.

[9] Barakat, M. and Hanke, T. (2012). Cryptography-Lecture Notes, Department of mathematics, University of Kaiserslautern, Germany.