Journal of Basic and Applied Engineering Research
p-ISSN: 2350-0077; e-ISSN: 2350-0255; Volume 2, Issue 19; October-December, 2015, pp. 1640-1643
© Krishi Sanskriti Publications
http://www.krishisanskriti.org/Publication.html

Date & Time Matrix Algorithm

Priti Gupta

Echelon Institute of Technology Faridabad, India
E-mail: guptapreet1989@gmail.com

Abstract—*In cryptography, encryption is the process of encoding messages in such a way that eavesdroppers or hackers cannot read it, but that authorized parties can. An authorized party, however, is able to decode the cipher text using a decryption algorithm that usually requires a secret decryption key. This paper contains an algorithm to encrypt the given time and date. By using these algorithms we can convert the time and date into some absurd form which cannot be traced by the hackers. In this paper, we using "Matrix Code" The matrix code uses various techniques like Fibonacci series, perfect number sequence and cumulation. It also uses a newly developed technique called "matrix symmetry" for development of matrix code. And this whole algorithm is known as "Time & Date-matrix algorithm".*

Keywords*:* *Time, Date***,** *Encryption, Fibonacci series, Symmetry, Perfect numbers, circular table arrangement, light wave pattern.*

1. INTRODUCTION

The encryption decryption has been used by humans to protect the secret information. In wartime, it has been used since early Times & Dates to transmit information from one location to another without being getting into the hand of enemies.

However in the era of information technology the scenario has changed because encryption has become vital for the common man also. For eg-Without encryption we can't think of protecting our bank accounts.

For the army it is essential to keep the information secret. The secret information in the war can make a huge difference and can be a reason for the victory. Hence for army encryption plays an important role. The strength of any encryption depends on how well it is able to keep the information safe and protected from any undesired party. There are several encryption algorithms which are available but are cumbersome.

However we can develop some of the simpler algorithms which can protect our information in a much simpler way. One such algorithm has been provided in this paper to encrypt the time and date. The encryption of time and date can be used for missile launches and attacks. These algorithms although being simple but at the same time can be effective too.

Cryptography is about constructing and analyzing protocols that block adversaries various aspects in information security such as data confidentiality, data integrity, authentication, and non-repudiation are central to modern cryptography. Modern cryptography exists at the intersection of the disciplines of mathematics, computer science, and electrical engineering. Applications of cryptography include ATM cards, computer passwords, and electronic commerce.

2. TIME & DATE ENCRYPT

The encrypt of time & date is an more important aspect during the wars because by doing so we can protect our information related to when we are going to attack and when we will launch a missile. Hence if we are able to protect the information about launching time or date we can simply be the side in advantage. This paper also provides one such simple and effective algorithm to encrypt the time & date.

Number Encryption

By time & date,form(HH:MM:SS&D:M) number refers to the N-digit unique number that is used to identify correct time & date. In date, year are not consider because There will be no need to encrypt the year. If we do so by some algorithm then the result can vary too much for example, if we encrypt 2015 by some way to 1970/ 2120 then it will make no sense as it has led to great variation from original year of event. But year are consider 4 digits identify the number code of the date & time number.

In the proposed algorithm, 8X8 matrix or a chess board is used for the development of matrix code. The center square is used for number code up to four digits. The second square from the center as shown in Fig. 1 is used for the date & time numbers up to twelve digits. The other squares are used to fill up the symmetry elements. p: date & time number ; c: number code.

Perfect Number

In number theory, a perfect number is a positive integer that is equal to the sum of its proper positive divisors, that is, the sum of its positive divisors excluding the number itself.

General solution: 2n *(2n+1 – 1); 1<n<infinity

Energy sequence in sub-shells of atom

Fig. 2 shows the energy sequence in increasing order, from 1s then 2s,2p,3s,3p,4s,3d,4p,5s and so on. In the algorithm proposed in this paper, numbers are assigned to the squares of the chess board in the energy sequence order. This sequence is also called aufbau’s principle.

Fibonacci Series
The first two numbers in the Fibonacci sequence is 0 and 1, depending on the chosen starting point of the sequence, and each subsequent number is the sum of the previous two. The series is:

0 1 1 2 3 5 8 13 21 34 55 89 144………

Cumulative frequency
Cumulative frequency can also defined as the sum of all previous frequencies up to the current point.

		P	**P**	**P**	**P**		
		P	**C**	**C**	**P**		
		P	**C**	**C**	**P**		
		P	**P**	**P**	**P**		

Fig. 1

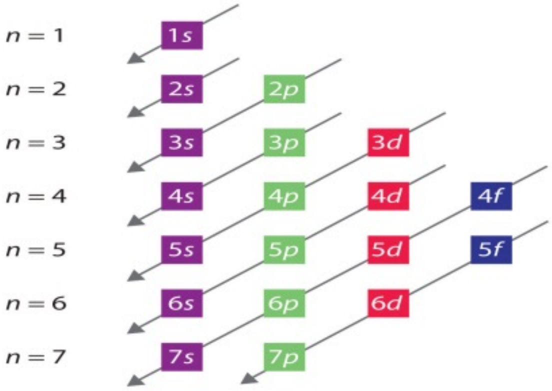


Fig. 2

Matrix Symmetry
The matrix symmetry is new concept developed for the distribution of numbers on a chess board. It is categorized into three types as α, β and γ symmetry. This type of symmetry mechanism is only valid for the elements of second square lying on the boundary of the square as shown in fig. 1.

α symmetry
This type of symmetry divides the element in the vertical direction. If the number n is even it is divided as (n/2, n/2) else it will be divided as ((n+1)/2, (n-1)/2). This symmetry will not work for corner elements.

α It is denoted as αRN or CN which means α -symmetry of Nth row or Nth column.

β symmetry
This type of symmetry divides the element in the horizontal direction. If the number n is even it is divided as (n/2, n/2) else it will be divided as ((n+1)/2, (n-1)/2). This symmetry will not work for corner elements.

It is denoted as β RN or CN which means β -symmetry of Nth row or Nth column.

γ-symmetry
This type of symmetry divides the element diagonally. If the number n is even it is divided as (n/2, n/2) else it will be divided as ((n+1)/2, (n-1)/2). This symmetry only works for corner elements. It is denoted as γ which means γ-symmetry of the corner elements.

This type of division of numbers through symmetry is done in the order of increasing energy sequence arrangement of numbers in the second square.

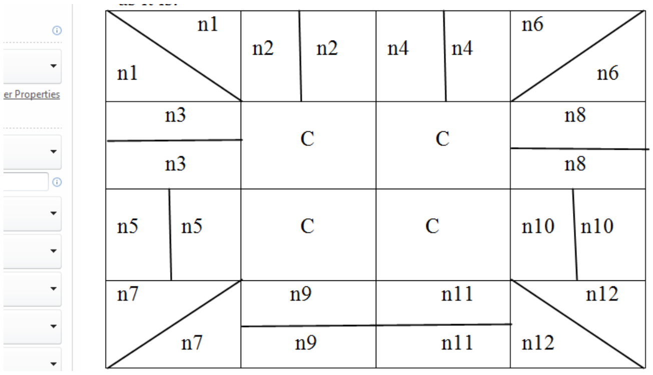
Only one type of code can be developed at a particular instant i.e. if code is based on row transition, the whole code should be based on row, similarly for the column transition.

For example: if the matrix code is

M-C: γ β R1 α R2 β R3 α R4

In fig. 3 the digits of the mobile number are arranged in the increasing sequence analogous to fig.2. As in the matrix code the corner elements are divided diagonally into equal parts as per even or odd number. Example the number N1 in the first box is divided diagonally to the first adjacent empty diagonal boxes.

Similarly the numbers in the other boxes except corner elements are divided into two equal parts and placed horizontally and vertically to the first adjacent empty boxes according to β and α symmetry respectively. If there is only one empty box in a particular direction the one half of the number will remain inside the box and if there is no empty box then the whole number will remain as it is.



n1 n1	n2 n2	n4 n4	n6 n6
n3 n3	C	C	n8 n8
n5 n5	C	C	n10 n10
n7 n7	n9 n9	n11 n11	n12 n12

Fig. 3

3. NUMBER ENCRYPT ALGORITHM

Consider that we have given the correct time of the form HH:MM: SS. Which we want to encrypt the below steps can be used to encrypt it.

i) Take the difference between Hours, Minutes and Seconds recursively. Keep taking (MM-HH) || (MM-SS). Until we get 0<MM-HH<24, 0<MM-SS<24.

ii) Now divide HH by (MM-HH) and represent it in form qr/|M-H|, q=quotient and r=remainder.

iii) We now ,we have (MM-HH),q , r and (MM-SS) and we can write like

|MM-HH|:qr:|MM-SS|

Consider that we have been give the date D/M/Y which we want to encrypt. The steps below can be used to encrypt.

i) Arrange the months in the tabular form in three groups of 31,30 ,28 days. In each group arrange the months in alphabetical orders.

Table 1

31	August
	December
	January
	July
	March
	May
	October
30	30 April
	June
	November
	September
29	29 February

ii) Now note the original date (D) and months (M).

iii) Now keep on doing D-11 till we obtain 0<D-11<11.

iv) Now form the circular table start counting form the month next to given months M till D-11.

Now we can take 10 number digit for more complex that data that by, We using K-Matrix Algorithm.

In K-Matrix Algorithm-

The encryption of data or time using K-Matrix algorithm is done.

i) First write the 10 number in the second square in the order of the energy sequence as shows.

ii) Now form section the number is the second square will divided according to Matrix code as shown in the fig.

iii) Then we rotate the value outside value in anticlockwise in one time. And then again calculate the value and get 10 number digits. Those are the encrypt value.

iv) The whole process can be reversed back to get the actual Date and Time.

4. ILLUSTRATIONS

In this section the above algorithm has been illustrated.

I 22:50:30 & 20-04-2015

i) MM-HH=> 50-22=28.
28-22=6.

ii) Number of steps=2

iii) HH/|MM-HH| => 22/6=5 ½. Hence q=3 and r=4.

iv) 6:34:20.

v) D=20 and M=April (4).

vi) Now keep doing D-11. 20-11=9<11.

vii) Now look into the Table.1. Start counting from the next month of the March till 9 hence we will get M'=March.

viii) Get Number=> 06:34:20&09:03. Put the number in K- matrix.

Table 2

0	6	4	0
3	2	1	9
2	0	5	3
0	0	0	0

Table 3

			0	0			
		1	0	0	5		
2	3	0	0	0	0	3	2
0	0	0			0	0	
1	1	0			0	1	2
		0	0	0	0		
		2	0	0	4		
			0	0			

xi) Then the center square will be rotated one time in the clockwise direction. This will give a new orientation of Number. This number also comes in the form of (HH:MM:SS&DD-MM).

Strength

The following reasons show the strength of this encryption algorithm-

i) The encrypted code also comes out to be in the form of number (time & date form), if not converted to letters, by which unauthorized party will think that they had obtained the correct time and will not try to decrypt it further.

ii) The large range of dates and months makes it strong.

iii) The use of circular table arrangement of month makes it unpredictable.

iv) The algorithm consists of simple steps which together develops an effective cipher.

v) The large range of hour, minute and second makes it stronger.

5. LIMITATION

This algorithm also has a limitation.

i) We obtains MM-HH =0 || MM-SS=0then this algorithm will not work as can be seen H/0 will not exist. Eg- 7:7, 11:11etc.

ii) Large variation in months can also cause problem. However we can come across the above limitations and can extend this algorithm by making some additional steps.

6. CONCLUSION

The above method shows that we can use the simpler steps to build an effective encrypted code. The improvement of the limitations of above algorithm could make them much strong encryption which we can use in encryption of missile launches, hidden projects etc. to surprise the enemy. The simple steps involved in these encryption makes the algorithm more flexible. The most important part of these algorithms is that the results don't seem to be encrypted by which we can make the enemy satisfy that it is not encrypted and he will not try to encrypt it.

REFERENCES

[1] Karan Kumar Singh. "Mobile number encryption using "K-matrix algorithm"", International Conference on Emerging Trends in Computational and Applied Mathematics (ICCAM-2014). PROCEEDINGS Department of Applied Science ITM University, Gurgaon (India).

[2] Ayush Jain, "Encryption of Time and Date", International Conference on Emerging Trends in Computational and Applied Mathematics (ICCAM-2014). PROCEEDINGS Department of Applied Science ITM University, Gurgaon (India).

[3] http://searchsecurity.techtarget.com/definition/encryption

[4] http://chem-guide.blogspot.in/2010/04/aufbau-principleand-bohr- bury-rule.html.

[5] R. Rivest, A. Shamir and L. Adleman., "A method for obtaining digital signatures and public key cryptosystems", Communications of the ACM, 1978; 21(2):120-126.

[6] T. Collins, D. Hopkins, S. Langford and M. Sabin, "Public key cryptographic apparatus and method", US Patent #5, 1997; 848;159.

[7] A.K.Lenstra, BM De Weger, "Twin RSA", Progress in Cryptology- MyCrypt 2005; 3715:222–228.

[8] S. Padhye, "On DRSA public key cryptosystem", International Arab Journal of Information Technology, 2006; 3(4):334-336.

[9] S. Sarkar, S. Maitra, "Cryptanalysis of Dual CRT-RSA", IACR Cryptology eprint 2010.

[10] S. Sarkar and S. Maitra, "Cryptanalytic results on Dual CRT-RSA and Common Prime RSA", Journal of Design and Codes Cryptography, 2013; 66:157-174.

[11] S. Golwasser, M. Micali, "Probabilistic Encryption", Journal of Computer and System Sciences, 1984; 28:270-299.