Quest Journals
Journal of Research in Applied Mathematics
Volume 9 ~ Issue 3 (2023) pp: 22-31
ISSN(Online) : 2394-0743 ISSN (Print): 2394-0735
www.questjournals.org

Research Paper

Encryption Technique of Concealing Highly Explosive Chemicals with Multiple Odd Magic Squares Constructions

[1.] Moirangthem Somoliya Devi, *TIITET, Bishnupur, Manipur,*
[2.] Salam Samarendra Singh, *Department of Mathematics, G.P. Women's College, Imphal, Manipur*
[3.] Longjam Jadumani Singh, *Department of Chemistry, Pettigrew College, Ukhrul, Manipur*

Abstract
In this paper, we try to find out a technique of concealing highly explosive chemicals which are the preserve of the military and the government defensive mechanism with the use of encryption technique by applying the odd magic to magic squares. In high explosives, such as RDX, TATB, the explosion propagates by a supersonic detonation, driven by the breakdown of the molecular structure of the material. An explosive can be characterized by the amount of energy it releases when detonated, as well as by its shearing and shock effect, or brisage. Here, we propose a specific rule of establishing odd magic to magic squares derived from odd Algebraic Latin squares and in turn magic to magic generation.
Key word: *RDX, TATB, Latin Squares, Magic Squares, RSA-encryption.*

Received 01 Mar., 2023; Revised 10 Mar., 2023; Accepted 12 Mar., 2023 © The author(s) 2023. Published with open access at www.questjournals.org

I. Introduction

The RSA public key cryptosystem [10] can be described briefly as follows:

(i) Consider two primes *p* and *q* (generally considered of same bit size, i.e. $q < p < 2q$).
(ii) $n = pq$ and $\phi(n) = (p - 1)(q - 1)$;
(iii) Select *e*, *d* such that $ed = 1 + k\,\phi(n)$, $k \geq 1$;
(iv) (*n*, *e*) are public key;
(v) (*n*, *d*) are private key;
(vi) Plaintext message *M* is encrypted as $C \alpha M^{e} \bmod n$;
(vii) For the decryption; ciphertext *C* is decrypted as $M \alpha C^{d} \bmod n$.

There may be many applications of the RSA-scheme; for an easy application of the RSA-scheme, the following highly explosive chemicals are considered.

Pyrotechnics are chemical technologies designed produce explosions, flames, smoke, or noise. Explosives are the most prominent pyrotechnic technology, not merely for useful in military purposes but for commercial ones, such as mining and construction, as well [1].

The term explosives are a specialized one and the term explosives means chemical materials to create an explosion. Explosive materials are used as bursting charges for bombs, missile warheads, grenades, and mines, and as propellants to fire bullets and artillery shells. They are used as blasting charges in military or commercial demolition, for earth-moving for engineering projects, and demolition of buildings and other structures. Explosives are categorized as low or high explosives. In low or deflagrating explosives, such as black powder, the explosion propagates through the material at subsonic speed through an accelerated burning or combustion process. In high explosives, such as RDX, TATB, the explosion propagates by a supersonic detonation, driven by the breakdown of the molecular structure of the material [2].

RDX is a heterocycle and has the molecular shape of a ring. It is an initialism for Research Department explosive [3]. It is an explosive nitroamine widely used in military and industrial applications. It was developed as an explosive which was more powerful than TNT(Trinitrotoulene) and it saw wide use in World War II. In its pure, synthesized state RDX is a white, crystalline solid. It is often used in mixtures with other explosives and plasticizers, phlegmatizers or desensitizers. RDX is stable in storage and is considered one of the most powerful and brisant of the military high explosives. The velocity of detonation of RDX at a density of 1.76 g/cm³ is 8750 m/s. It burns rather than explodes and detonates only with a detonator, being unaffected even by small arms fire [4].

Preparation

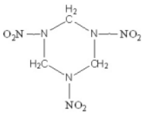
It is obtained by reacting white fuming nitric acid (WFNA) with hexamine, producing dinitromethane and ammonium nitrate as byproducts [5].

Reaction

$(CH_2)_6N_4 + 10HNO_3 \rightarrow (CH_2\text{-}N\text{-}NO_2)_3 + 3CH_2(NO_2)_2 + NH_4NO_3 + 3H_2O$

Hexamine nitric acid RDX dinitromethane ammonium nitrate water

Structure



Structure of RDX

IUPAC Name: 1, 3, 5-Trinitroperhydro-1, 3, 5-triazine

Molecular formula: $C_3H_6N_6O_6$

TATB is an aromatic explosive, based on the basic six-carbon benzene ring structure with three nitro functional groups (NO_2) and three amine (NH_2) groups attached, alternating around the ring. TATB is a powerful explosive (somewhat less powerful than RDX, but more than TNT), but it is extremely insensitive to shock, vibration, fire, or impact. Because it is so difficult to detonate by accident, even under severe conditions, it has become preferred for applications where extreme safety is required, such as the explosives used in nuclear weapons, where accidental detonation during an airplane crash or rocket misfiring would present extreme dangers [6].

TATB has been found to remain stable at temperatures at least as high as 250°C for prolonged periods of time. TATB is a bright yellow colour. At a pressed density of 1.80, TATB has a velocity of detonation of 7,350 meters per second. TATB has a crystal density of 1.93 grams/cm^3.

Preparation

TATB is produced by nitration (a mixture of concentrated nitric acid and concentrated sulphuric acid, catalyst) of 1,3,5-trichlorobenzene to 1,3,5-trichloro-2,4,6-trinitrobenzene, then the chlorine atoms are substituted with amine groups [7].

Reaction

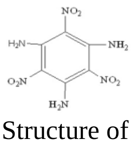
$$C_6H_3Cl_3 + 3HNO_3 \xrightarrow[330K]{H_2SO_4} C_6(NO_2)_3Cl_3 + 3H_2O$$

1,3,5-trichlorobenzene nitric acid 1,3,5-trichloro-2,4,6-trinotrobenzene water

$$C_6(NO_2)_3Cl_3 + 3NH_3 \xrightarrow{443K} C_6(NO_2)_3(NH_2)_3 + 3HCl$$

1,3,5-trichloro-2,4,6-trinotrobenzene ammonia TATB hydrochloric acid

Structure



Structure of TATB

IUPAC Name: 1,3,5-triamino-2,4,6-trinitrobenzene

Molecular formula: $C_6H_6N_6O_6$

1.1 Magic Square and Public-Key Cryptosystem

There is a specific rule of establishing odd magic squares derived from odd Algebraic Latin squares. Magic Squares are practically important from the properties of its equality in the sum of its rows, columns, diagonals, etc. Since the magic squares (*n* x *n*) exist for odd numbers of rows, columns and diagonals only. It can be used in cryptographic analysis as encryption keys for developing magic square ciphers.

We propose the application of encryption algorithm with the help of Odd Magic to Magic Squares is very helpful in concealing these explosives secret. Cryptography is the science of keeping secrets secret. Further, magic square encryption is becoming one of the fascinating techniques. As an alternative approach to handling the explosive compounds which have the components of C-atoms, H-atoms, N-atoms and O-atoms respectively

particularly in RDX and TATB with the encoding process of ASCII characters in the cryptosystems had been thought of in this work. It can also be applicable to all the remaining explosives.
There has been a lot of interest in the construction of safe and effective public key cryptosystems, which ensure the security of the data [8]. The basic idea of a public key cryptosystem is due to Diffie and Hellman [9]. To set up an RSA-Cryptosystem, one must be able to recognize easily whether large numbers are primes or not and make their product $n = pq$ public. n is part of the public key, whereas the factors p and q of n are kept secret and are used as the secret key. The basic idea is that the factors of n cannot be converted from n. Rivest, Shamir and Adleman recommended that n be about 200 digits long key, that is one needs longer key to have more secure [10]. Longer or shorter lengths can be used depending on the relative importance of encryption speed and security in the application at hand. An 80-digit n provides moderate security against an attack using current technology; using 200 digits provides a margin of safety against future developments.
The public-key consists of the modulus $n = pq$, and an exponent e such that $d = e^{-1} \bmod (p-1)(q-1)$. To encrypt a plaintext M the user computes $C = M^e \bmod n$ and to decrypt we get the plaintext by calculating $M = C^d \bmod n$. In order to thwart currently known attacks, the modulus n and thus M and C should have a length of 512-1024 bits [10].

II. Methodology

The working methodology of the proposed add-on security of Odd Magic to Magic Square Encryption is discussed as the following subsections.

2.1 Basic Latin Square

Let us consider a 3 × 3 odd Latin square with the elements of $a_{11}, a_{12}, \cdots, a_{33}$.
Representing the above in algebraic form of Latin Square, we have

$$\begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{22} & a_{23} & a_{21} \\ a_{33} & a_{31} & a_{32} \end{bmatrix}$$

Fig. 1(a). Algebraic form of Latin Square

Which can be written as

$$\begin{bmatrix} 1 & 2 & 3 \\ 5 & 6 & 4 \\ 9 & 7 & 8 \end{bmatrix}$$

Fig. 1(b). Latin Square 3×3

In all cases the Latin letters are seen once in each row and column. Here, the sums of all columns are equal but not the sum of the diagonals i.e. $\sum_i d_{ij} \neq \sum_j d_{ij}$, where $a_{11} \neq a_{21} \neq \cdots \neq a_{33}$ and so on. Then the ultimate normal magic square of 3 × 3 is

$$\begin{bmatrix} 8 & 1 & 6 \\ 3 & 5 & 7 \\ 4 & 9 & 2 \end{bmatrix}$$

Fig. 1(c). Normal Magic Square of 3 × 3

2.2 Construction of Odd Magic Squares

Odd magic square is defined as the magic square where the number of columns as well as the number of rows in a matrix becomes odd. The working principle of magic square construction is discussed stepwise [11]. The following three steps of odd ordered magic squares are discussed as

(i) Consecutive natural numbers 1 to n^2 in n rows and n columns are inserted. Find out the values of pivot element $P = \dfrac{1+n^2}{2}$ and the magic sum, $S = \dfrac{n(1+n^2)}{2}$.
(ii) Arrange the $n*n$ matrix in Basic Latin Square to get the column sums equal.
(iii) Select the row associated with P, assign this row as main diagonal elements (keeping the pivot element in the middle cell) in ascending order or descending order and arrange other (column) elements in an orderly manner to get the desired magic square.

In consequence to the above steps, the Basic Latin Square of 5 × 5 matrix is constructed as in Figure 2.

$$\begin{bmatrix} a_{11} & a_{12} & a_{13} & a_{14} & a_{15} \\ a_{22} & a_{23} & a_{24} & a_{25} & a_{21} \\ a_{33} & a_{34} & a_{35} & a_{31} & a_{32} \\ a_{44} & a_{45} & a_{41} & a_{42} & a_{43} \\ a_{55} & a_{51} & a_{52} & a_{53} & a_{54} \end{bmatrix}$$

Fig. 2. Algebraic form of Latin Square

Once the algebraic form of Latin Square is constructed in n^2, then the arrangement of the first magic square is simple. In the above Figure 2, a_{33} is the pivot element. Representing the pivot element in the middle cell of the 5 × 5 matrix, we have,

		a_{11}		a_{35}
		a_{22}	a_{34}	
	a_{32}	a_{44}		
a_{31}	a_{43}	a_{55}		

Fig. 3. Pivot element in the middle cell

Select the column containing a_{33} and insert in the middle column of the 5 × 5 matrix as performed in Figure 2. Then, we can set up as $\lfloor a_{33} \quad a_{44} \quad a_{55} \quad a_{11} \quad a_{22} \rfloor$ in the third column i.e. the pivot column.

Again, selecting the column containing a_{34} and arrange as $\lfloor a_{34} \quad a_{45} \quad a_{51} \quad a_{12} \quad a_{23} \rfloor$. Similarly, for the columns containing a_{35}, a_{31} and a_{32} we can arrange like $\lfloor a_{35} \quad a_{41} \quad a_{52} \quad a_{13} \quad a_{24} \rfloor$, $\lfloor a_{31} \quad a_{42} \quad a_{53} \quad a_{14} \quad a_{25} \rfloor$ and $\lfloor a_{32} \quad a_{43} \quad a_{54} \quad a_{15} \quad a_{21} \rfloor$. Finally, we obtain a 5 × 5 magic square as

a_{42}	a_{54}	a_{11}	a_{23}	a_{35}
a_{53}	a_{15}	a_{22}	a_{34}	a_{41}
a_{14}	a_{21}		a_{45}	a_{52}
a_{25}	a_{32}	a_{44}	a_{51}	a_{13}
a_{31}	a_{43}	a_{55}	a_{12}	a_{24}

Fig. 4. Algebraic Magic Square of 5 × 5

It can be simplified with a numerical example of a 5 × 5 magic square with the integers 1, 2, 3, ⋯, 25 as the following.

$$\begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 7 & 8 & 9 & 10 & 6 \\ 13 & 14 & 15 & 11 & 12 \\ 19 & 20 & 16 & 17 & 18 \\ 25 & 21 & 22 & 23 & 24 \end{bmatrix}$$

Fig. 5. Magic Square of 5 × 5

Now, $\frac{n^2+1}{2}$ i.e. $\frac{25+1}{2}$ = 13 represents the pivot element keeping row in the diagonal of the 5 × 5 matrix, we have,

17	24	1	8	15
23	5	7	14	16
4	6		20	22
10	12	19	21	3
11	18	25	2	9

Fig. 6. Magic Square of 5 × 5

The constant sum in every row, column and diagonal in the above odd magic square is 65 and it is called the magic constant or magic sum.

2.3 Construction of 13 × 13 Odd Magic Square

We construct a 13×13 odd magic square so that one can encode any element from the periodic table by comparing with the existing Partial ASCII – Unicode Table 1. The odd magic square of 13×13 is so constructed because most of the elements in periodic table belong in the atomic range of 13×13 i.e. 169. We follow the same protocol what we have performed in Section 2.2. First, we construct the Basic Latin Square of the integers 1, 2, 3, ···, 169 in 13×13 as in Figure 7.

1	2	3	4	5	6	7	8	9	10	11	12	13
15	16	17	18	19	20	21	22	23	24	25	26	14
29	30	31	32	33	34	35	36	37	38	39	27	28
43	44	45	46	47	48	49	50	51	52	40	41	42
57	58	59	60	61	62	63	64	65	53	54	55	56
71	72	73	74	75	76	77	78	66	67	68	69	70
	86	87	88	89	90	91	79	80	81	82	83	84
99	100	101	102	103	104	92	93	94	95	96	97	98
113	114	115	116	117	105	106	107	108	109	110	111	112
127	128	129	130	118	119	120	121	122	123	124	125	126
141	142	143	131	132	133	134	135	136	137	138	139	140
155	156	144	145	146	147	148	149	150	151	152	153	154
169	157	158	159	160	161	162	163	164	165	166	167	168

Fig. 7. Basic Latin Square 13×13

Now, the pivot element $P=\frac{13^2+1}{2}$ i.e. $P=\frac{169+1}{2}$ = 85 and fixing the column which includes the pivot element in the middle column i.e. in the 7th column and represent the other elements according to Section 2.2. Finally, we get the magic square of the sum

Fig. 8. MS_1 of 13×13

$S=\frac{13(1+13^2)}{2}=1105$ in each column, row and diagonals respectively. The construction of magic squares of 13×13 can encode most of the atoms involved in the above mentioned chemicals. One can construct magic squares bigger than 13×13 if necessity of more security demands.

93	108	123	138	153	168	1	16	31	46	61	76	91	**1105**
107	122	137	152	167	13	15	30	45	60	75	90	92	**1105**
121	136	151	166	12	14	29	44	59	74	89	104	106	**1105**
135	150	165	11	26	28	43	58	73	88	103	105	120	**1105**

149	164	10	25	27	42	57	72	87	102	117	119	134	**1105**
163	9	24	39	41	56	71	86	101	116	118	133	148	**1105**
8	23	38	40	55	70		100	115	130	132	147	162	**1105**
22	37	52	54	69	84	99	114	129	131	146	161	7	**1105**
36	51	53	68	83	98	113	128	143	145	160	6	21	**1105**
50	65	67	82	97	112	127	142	144	159	5	20	35	**1105**
64	66	81	96	111	126	141	156	158	4	19	34	49	**1105**
78	80	95	110	125	140	155	157	3	18	33	48	63	**1105**
79	94	109	124	139	154	169	2	17	32	47	62	77	**1105**
1105	**1105**	**1105**	**1105**	**1105**	**1105**	**1105**	**1105**	**1105**	**1105**	**1105**	**1105**	**1105**	**1105**

And Figure 8 is the first Odd Magic Square of 13×13 formed by using the Latin Square format.

2.4 Construction of Odd Magic to Magic Square Matrices

The first so formed magic square is termed as Base-Magic Square and it is denoted by MS_1 as in section 2.2. The working model of odd magic to magic square construction is discussed stepwise [14]. The first column of MS_1 becomes the pivot column of the second magic square which is denoted by MS_2.

The followings are the steps of odd magic to magic square:

(i) Consecutive natural numbers 1 to n^2 in n rows and n columns are inserted. Find out the values of pivot element $P = \frac{1+n^2}{2}$ and the magic sum, $S = \frac{n(1+n^2)}{2}$.

(ii) Arrange the $n*n$ matrix in Basic Latin Square to get the column sums equal.

(iii) Select the row associated with P, assign this row as main diagonal elements (keeping the pivot element in the middle cell) in ascending order or descending order and arrange other (column) elements in an orderly manner to get the desired magic square.

(iv) Assign the first magic square so constructed as MS_1 and elements of MS_1 as $n*n$ matrix similar to the previous Basic Latin Square.

(v) Insert the first column of MS_1 as the pivot column in MS_2 and the elements of MS_1 in the cells of $a_{(\frac{n+1}{2})2}, a_{(\frac{n+1}{2})3}, \dots, a_{(\frac{n+1}{2})(\frac{n+1}{2})}$ will replace the diagonal cells of MS_2 as $a_{(\frac{n+1}{2}-1)(\frac{n+1}{2}+1)}, a_{(\frac{n+1}{2}-2)(\frac{n+1}{2}+2)}, \dots, a_{1n}$ and the row elements $a_{(\frac{n+1}{2})(\frac{n+1}{2}+1)}, a_{(\frac{n+1}{2})(\frac{n+1}{2}+2)}, \dots, a_{(\frac{n+1}{2})n}$ on the right of pivot element of MS_1 will replace the lower diagonal cells of MS_2 as $a_{n1}, a_{(n-1)2}, \dots, a_{(\frac{n+1}{2}+1)(\frac{n+1}{2}-1)}$.

(vi) Repeat step (iii) till all the vacant cells of MS_2 are filled up as performed in Basic Latin Square.

In consequence to the above 6 steps, the Odd Magic to Magic Square of 13×13 matrix is constructed as in Figure 9.

114	143	159	19	48	77	93	122	151	11	27	56	85	**1105**
128	144	4	33	62	91	107	136	165	25	41	70	99	**1105**
142	158	18	47	76	92	121	150	10	39	55	84	113	**1105**
156	3	32	61	90	106	135	164	24	40	69	98	127	**1105**
157	17	46	75	104	120	149	9	38	54	83	112	141	**1105**
2	31	60	89	105	134	163	23	52	68	97	126	155	**1105**
16	45	74	103	119	148		37	53	82	111	140	169	**1105**
30	59	88	117	133	162	22	51	67	96	125	154	1	**1105**
44	73	102	118	147	7	36	65	81	110	139	168	15	**1105**
58	87	116	132	161	21	50	66	95	124	153	13	29	**1105**
72	101	130	146	6	35	64	80	109	138	167	14	43	**1105**
86	115	131	160	20	49	78	94	123	152	12	28	57	**1105**
100	129	145	5	34	63	79	108	137	166	26	42	71	**1105**

1105	**1105**	**1105**	**1105**	**1105**	**1105**	**1105**	**1105**	**1105**	**1105**	**1105**	**1105**	**1105**	**1105**

Fig. 9. MS_2 of 13×13

3. Magic Square Implementation in Public-Key Cryptosystem

For encryption of a message, one needs the Unicode Table to understand the proper number code assigned to every characters. The characters and their associated number code are listed in the Table 1. The first 32 characters (0 through 31) are nonprintable characters, and character #32 is the space. Therefore, they are not shown in the table below.

Table 1. Partial ASCII – Unicode Table

33 !	34 ”	35 #	36 $	37 %	38 &	39 ’	40 (	41)	42 *
43 +	44 ,	45 -	46 .	47 /	48 0	49 1	50 2	51 3	52 4
53 5	54 6	55 7	56 8	57 9	58 :	59 ;	60 <	61 =	62 >
63 ?	64 @	65 A	66 B	67 C	68 D	69 E	70 F	71 G	72 H
73 I	74 J	75 K	76 L	77 M	78 N	79 O	80 P	81 Q	82 R
83 S	84 T	85 U	86 V	87 W	88 X	89 Y	90 Z	91[	92 \
93]	94 ^	95 _	96 ‘	97 a	98 b	99 c	100 d	101 e	102 f
103 g	104 h	105 i	106 j	107 k	108 l	109 m	110 n	111 o	112 p
113 q	114 r	115 s	116 t	117 u	118 v	119 w	120 x	121 y	122 z
123 {	124 |	125 }	126 ~						

There are two basic approaches used to speed up the cryptographic transformations for concealing the highly explosive chemicals. The first approach is to design faster (symmetric or asymmetric) cryptographic algorithms. This approach is not available most of the time. The speed of cryptographic algorithm is typically determined by the number of rounds (in private-key) or by the size of messages (in public-key case). The second case is the parallel cryptographic system. The main idea is to take a large message block [8].

In Ganapathy and Mani’s paper [12], the algorithm starts with building 4 × 4 magic square. Incrementally 8 × 8 and 16 × 16 (even magic squares) magic squares are built using 4 × 4 magic squares as building blocks. While constructing the doubly even magic squares the following block is used as the first constructing block.

-4	MS_{start}	-8	+12
-10	+14	-6	+2
+8	-12	+4	$MST4_{sum}$
+6	-2	+10	-14

Fig. 10. Magic Square filling order

where MS_{start} = starting number of MS, $MST4_{sum}$ = Total sum of MS of order 4; -int represents the places to fill the values in MS, starting from $MST4_{sum}$ and decremented by 2 each time, and +int represents the places to fill the values in MS, starting from MS_{start} and incremented by 2 each time to get the next number [12].

Here, we develop an odd 13 × 13 magic square and check the security of encryption for sending messages. First, we construct the Latin Square of elements 1, 2, 3, ..., 169 as in the above figure 8 and 9.

Following the steps of section 2.3, the first so formed magic square is termed as Base-Magic Square and denoted by MS_1. The first column of MS_1 will become the pivot column of the second MS_2. Then, the pivot row having the cells $\lfloor a_{72} \quad a_{73} \quad a_{74} \quad a_{75} \quad a_{76} \quad a_{77} \rfloor$ will become the diagonal cells above the pivot cells i.e. these will occupy $\lfloor a_{68} \quad a_{59} \quad a_{410} \quad a_{311} \quad a_{212} \quad a_{113} \rfloor$ as inserted in the MS_2 and $\lfloor a_{78} \quad a_{79} \quad a_{710} \quad a_{711} \quad a_{712} \quad a_{713} \rfloor$ will occupy the position of the cells

$\lfloor a_{131} \quad a_{122} \quad a_{113} \quad a_{104} \quad a_{95} \quad a_{86} \rfloor$ respectively. Bah! Still the sums of all the rows, columns and diagonals have the same sum 1105. The magic square MS_2 is obtained by interchanging the cell elements of MS_1 as stated above in the section 2.3. If we go on in this process, we will be convenient to construct a number of magic squares. If such number of magic squares are constructed and encode different atoms according to the number of atoms attached to the compound, it will be more secure. In this paper, only four MS_j matrices are generated. Other matrices can be generated by taking the same process as we have presented.

To show the relevance of this work to the security of public-key encryption schemes, a public-key cryptosystem RSA is taken.

For a proper understanding, let us select two prime numbers, $p = 3$ and $q = 11$ for an easy calculation. We calculate $n = pq = 3 \times 11 = 33$. Then, we calculate $\boldsymbol{\phi}(n) = (p - 1)(q - 1) = 2 \times 10 = 20$. Now, let us select e such that e is relatively prime to $\boldsymbol{\phi}(n) = 20$ and less than $\boldsymbol{\phi}(n)$; we choose $e = 7$. We determine d such that $de \equiv 1$ mod 20 and $d < 20$. The correct value of $d = 3$, because $7 \times 3 = 21 = 2 \times 10 + 1$; d can be calculated using the extended Euclid's algorithm. The resulting keys are public key $K_U = \{n, e\} = \{33, 7\}$ and private key $K_R = \{n, d\} = \{33, 3\}$. To encrypt a message, using eq. $C = M^7$ mod 33 and to decrypt the same, we use the eq. $M = C^3$ mod 33 are used.

Here, the message to be encrypted is $C_3H_6N_6O_6$ (RDX). The encoded message due to the ASCII in Table 1 for C_3, H_6, N_6 and O_6 are [151 81 45 131] by comparing from the magic square tables provided according to the number of atoms attached to the respective elements. The plaintext of C_3 is 151 as occurred in the 3rd generated magic square in Figure 11.

51	81	124	167	28	71	114	144	18	61	104	134	8
65	95	138	12	42	85	128	158	32	75	105	148	22
66	109	152	26	56	99	142	3	46	89	119	162	36
80	123	166	27	70	113	156	17	60	103	133	7	50
94	137	11	41	84	127	157	31	74	117	147	21	64
108	151	25	55	98	141	2	45	88	118	161	35	78
122	165	39	69	112	155		59	102	132	6	49	79
136	10	40	83	126	169	30	73	116	146	20	63	93
150	24	54	97	140	1	44	87	130	160	34	77	107
164	38	68	111	154	15	58	101	131	5	48	91	121
9	52	82	125	168	29	72	115	145	19	62	92	135
23	53	96	139	13	43	86	129	159	33	76	106	149
37	67	110	153	14	57	100	143	4	47	90	120	163

Fig. 11. 3rd generated Magic Square MS_3

But the other atoms occur in 6th generated magic square as they have 6 atoms each. Their plaintexts are 81, 45 and 131 respectively in Figure 12.

60	132	48	120	36	108	24	96	12	84	169	72	144
74	146	62	134	50	122	38	110	26	98	1	86	158
88	160	76	148	64	136	52	124	27	112	15	100	3
102	5	90	162	78	150	53	138	41	126	29	114	17
116	19	104	7	79	164	67	152	55	140	43	128	31
130	33	105	21	93	9	81	166	69	154	57	142	45
131	47	119	35	107	23		11	83	168	71	156	59
145	61	133	49	121	37	109	25	97	13	85	157	73
159	75	147	63	135	51	123	39	111	14	99	2	87

4	89	161	77	149	65	137	40	125	28	113	16	101
18	103	6	91	163	66	151	54	139	42	127	30	115
32	117	20	92	8	80	165	68	153	56	141	44	129
46	118	34	106	22	94	10	82	167	70	155	58	143

Fig. 12. 6^{th} generated Magic Square MS_6

The encryption is done by taking the above prime numbers as mentioned earlier. One such process of encryption and decryption in C_3 can be performed as the following Figure 13.

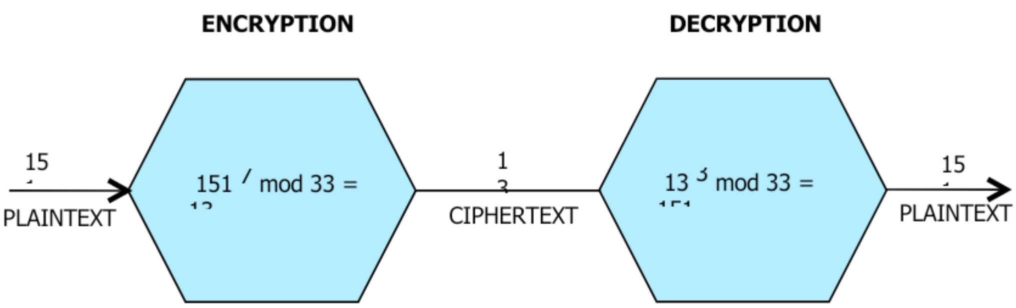


Fig. 13. Encryption and decryption of C3

The scheme is like this, to encrypt C_3, the numerals which occur at 67^{th} position in the 3^{rd} generated magic square MS_3 in Figure 11 is taken i.e. 151 because C occurs only in the first position of the clear text having 3 atoms. Similarly, to encrypt H_6, N_6 and O_6, the numerals occur in the 72^{nd}, 78^{th} and 79^{th} positions of the 6^{th} generated magic square MS_6 as in Figure 12 respectively are taken.

Thus, $M_1(C_3) = 151$, $M_2(H_6) = 81$, $M_3(N_6) = 45$, and $M_4(O_6) = 131$ respectively according to the position of letters in figures 10 and 11. Hence, the encryptions are done as in [10], $C_1(C_3) = 151^7 \bmod 33 = 13$, $C_2(H_6) = 81^7 \bmod 33 = 27$ and $C_3(N_6) = 45^7 \bmod 33 = 12$ and $C_3(O_6) = 131^7 \bmod 33 = 32$. Thus, the encrypted message of Alice is [13 27 12 32].

Again, when Bob wishes to decrypt the above encryption, he will use the private key (n, d) and for decryption, $M = C^d \pmod n$. Then $M_1(C_3) = 13^3 \bmod 33 = 151$, $M_2(H_6) = 27^3 \bmod 33 = 81$ and $M_3(N_6) = 12^3 \bmod 33 = 45$ and $M_3(O_6) = 32^3 \bmod 33 = 131$ i.e. the original text-message which was sent by Alice is $C_3H_6N_6O_6$.

In the way we performed above, the encryption and decryption of $C_6H_6N_6O_6$ (TATB) can be worked out easily as follows:

Here, to encrypt C_6, H_6, N_6 and O_6, the numerals occur in the 67^{th}, 72^{nd}, 78^{th} and 79^{th} – all the atoms occur only in the 6^{th} generated magic square MS_6. Their encoded numerals are [33 81 45 131] taken as in Figure 11. The exception to the above encryption and decryption occurs in the case of C-atoms only, that also falls in MS_6.

The encryption and decryption of C_6 can be performed as $C_1(C_6) = 33^7 \bmod 33 = 0$ and $M_1(C_6) = 0^3 \bmod 33 = 33$. Therefore, the encrypted message is [00 27 12 32]. When decrypted the above message by Bob, it is transformed into the plaintext as [33 81 45 131]. Further, it is observed that if the file size increased, then encryption and decryption time will also be increased.

III. Conclusion.

The Security Model for Public-Key Cryptosystem based on Magic Square will increase the security due to its complexity in encryption because it deals with the magic square formation with Base-Magic Square and sum of the columns, rows and diagonals that cannot be easily traced out. But it will be more complicated in the case of Odd Magic to Magic Squares because there has more complexity to trace out the pivot element and elements to be filled up in the remaining cells in such magic squares. The encryption/decryption is based on cell numerals generated by magic square rather than the ASCII values. Due to its importance and its beautiful, simple structure, the RSA scheme has also attracted many cryptanalysts [13]. But despite intensive research efforts, from a mathematical point of view the only known method to break the RSA scheme is the most obvious one, i.e. to find the factorization of *n*.

An alternative approach to the existing ASCII based cryptosystem a number based approach is thought of and implemented in the highly explosive chemicals. The technique so developed in this paper is a complicated one by exploring the odd magic to magic square encryption which is applicable to any C-atom present in the explosive compounds.

REFERENCES:

[1]. Akhavan, Jacqueline, The Chemistry of Explosives, Cambridge, UK: Royal Society of Chemistry, ISBN 0-85404-640-2, (2004)

[2]. Davis, Tenney L., The Chemistry of Powder and Explosives II, New York: John Wiley & Sons Inc., (1943)

[3]. Luo, K.-M., Lin, S.-H., Chang, J.-G., Huang, T.-H., "Evaluations of kinetic parameters and critical runaway conditions in the reaction system of hexamine-nitric acid to produce RDX in a non-isothermal batch reactor", Journal of Loss Prevention in the Process Industries, 15 (2): pp. 119–127, doi:10.1016/S0950-4230(01)00027-4, (2002)

[4]. Department of the Army Technical Manual TM 9-1300-214: Military Explosives. Headquarters, Department of the Army, United States.

[5]. Bachmann, W. E.; Sheehan, John C., "A New Method of Preparing the High Explosive RDX", Journal of the American Chemical Society, 71 (5): pp. 1842–1845, doi:10.1021/ja01173a092, May, (1949)

[6]. Cooper, Paul W., Explosives Engineering, New York: Wiley-VCH, ISBN 0-471-18636-8, (1996)

[7]. Hale, George C., "The Nitration of Hexamethylenetetramine", Journal of the American Chemical Society, 47 (11): pp. 2754–2763, doi:10.1021/ja01688a017, November, (1925)

[8]. Abisha P.J., Thomas D.G., Subramanian K.G.: Public Key Cryptosystems Based on Free Partially Commutative Monoids and Groups. INDOCRYPT, pp. 218-227, (2003)

[9]. Diffie W., Hellman M.: New directions in cryptography. IEEE Transactions on Information Theory, Vol. IT-22, 6; pp. 644-654, (1976)

[10]. Rivest R. L., Shamir A. and Adleman L.: A method for Obtaining digital signatures and Public-Key Cryptosystems. Communications of the ACM, 21(2): pp. 120-126, February, (1978)

[11]. Tomba I.: A Technique for constructing Odd-order Magic Squares using Basic Latin Squares, International Journal of Scientific and Research Publications, Vol-2, pp. 550-554, May (2012)

[12]. Ganapathy G., Mani K.: Add-On Security Model for Public-Key Cryptosystem Based on Magic Square Implementation. Proceedings of the World Congress on Engineering and Computer Science 2009 Vol I., WCECS, San Francisco, USA, (2009)

[13]. Hall C., Golberg I., and Schneir B.: Reaction Attacks Against Several Public Key Cryptosystems. Proceedings of ICICS 1999, LNCS 1726, pp. 2-12. Springer-Verlag, (1999)

[14]. Salam S. & Moirangthem S: Construction of Multiple Odd Magic Squares. Asian Journal of Mathematics & Computer Research, 29(1): pp. 42-52, May, (2022)