Kirkuk University Journal /Scientific Studies (KUJSS)
Volume 12, Issue 4, September 2017
ISSN 1992 – 0849

An Improved RSA based on Double Even Magic Square of order 32

Shahla Uthman Umar-college of science- University of Kirkuk

Shahla_umar@uokirkuk.edu.iq

Shahla_aothman@yahoo.com

[Abstract]

Because of the computers systems discovery and the use of computer networks between countries, security is very important to transfer confidential information over the networks; traditional cryptographic systems such as Rivest-Shamir-Adlemen (RSA) are depend on guesswork as well as mathematics. Information theory illustrates that conventional cryptographic systems cannot be regarded fully secure unless the private key ; which it is used once only ; is at least as long as the plain text. And another limitation is using ASCII value to represent the plaintext, So the repetition of characters in the plain text will appear in the cipher text therefore we have given approach to generate magic square of order 32 which cannot be easily traced and use this square in the cryptography which it is used to improve efficiency through providing an additional level of security to encryption. Through of the characteristics of magic squares, and it's some complex conditions (non-repetition property), these squares generates a huge numbers of non-duplicate random numbers which can be used to represent the numerals rather than ASCII values as well as the magic square is also used to generate the keys for public key encryption algorithms.

[Keywords: Magic Square, RSA, Public Key Cryptosystem, Encryption algorithm, key.]

تحسين خوارزمية التشفير RSA بأستخدام المربعات السحرية الفردية المزدوجة ذات المرتبة ٣٢

شهلة عثمان عمر – كلية العلوم –جامعة كركوك

Shahla_umar@uokirkuk.edu.iq

Shahla_aothman@yahoo.com

الملخص

بسبب اكتشاف أنظمة الحواسيب واستخدام شبكات الحاسوب بين البلدان، فإن امن البيانات مهم جدا لنقل المعلومات السرية عبر الشبكات ، واكثر أنظمة التشفير التقليدية مثل (RSA) تعتمد على التخمين بالاضافة الى الرياضيات. توضح نظرية المعلومات أن أنظمة التشفير التقليدية لا يمكن اعتبارها آمنة تماما إلا إذا كان المفتاح الخاص والتي يتم استخدامها مرة واحدة فقط على الأقل بطول النص الصريح. ومن القيود الاخرى في هذه الطريقة هو استخدام قيمة (ASCII) لتمثيل النص الصريح، وبالتالي فإن تكرار الأحرف في النص الصريح سوف تظهر في النص المشفر لذلك اقترحنا طريقة جديدة لتوليد المربعات السريعة ذات المرتبة ٣٢ والتي لا يمكن تتبعها والتنبوء بقيمها بسهولة واستخدام هذه المربعات في التشفير والذي يستخدم لتحسين كفاءة التشفير من خلال توفير مستوى إضافي من الأمان . من خلال خصائص المربعات السحرية، وبعض شروطها المعقدة (مثل خاصية عدم التكرار للقيم)، هذه المربعات تولد أعدادا كبيرة من الأرقام العشوائية غير المكررة والتي يمكن استخدامها لتمثيل الأرقام بدلا من القيم (ASCII)، وكذلك المربعات السحرية تستخدم أيضا لتوليد مفاتيح خوارزميات التشفير بالمفتاح العام.

الكلمات المفتاحية:- المربع السحري، نظام التشفير بالمفتاح العام، خوارزمية التشفير، [المفتاح]

1. Introduction

Cryptography pointed completely on encryption, which is the process of transforming original information ([plaintext]()) into unreadable text ([cipher text]()), while

Kirkuk University Journal /Scientific Studies (KUJSS)
Volume 12, Issue 4, September 2017
ISSN 1992 – 0849

decryption is the inverse, Converting from the unreadable cipher text back to plaintext. In cipher, there are two algorithms, the encryption and the reversing decryption [1].

There are two kinds of cryptosystems, symmetric and asymmetric. In asymmetric systems there are two keys, the first one (public key) is used to encrypt a message while the second one (private key) is used to decrypt it, therefore these systems increase the security of communication [1]. An example of asymmetric systems is RSA, The security of several cryptographic systems relates with the creation of unexpected elements like the secret key in the DES algorithms, the key stream in the one-time pad and the prime P, and Q in the RSA encryption. In every these instances, the keys made must be sufficient in size and the arbitrary. However, RSA is not completely secure or secure against chosen cipher text attacks. If all variables are selected in such a way that it's impossible to compute the private key (d) from the public key (n, e), or choosing P, Q are incredibly large. Even if the above variables were selected carefully, none of the computational problems are completely guaranteed enough [2]. To encrypt the clear message characters, their ASCII values are taken which is possible that the same cipher text is produced for the characters which occur in several positions in the plaintext**.** To eliminate this problem, this paper attempts to improve a method with "doubly even magic squares (DEMS)" of order 32 (32 ×32) which equals to 1024 different values and dividing this magic square to different corresponding ASCII tables (each table is 128 ASCII characters). Thus, instead of taking the ASCII values of the characters to encrypt, different numerals representing the location of ASCII values in the magic square are taken and also using the same magic square to select two prime numbers (P and Q) which is used to generate the public key (e, n) then these numerals are encrypted using "RSA cryptosystem".

2. Related Work

As the intruder has the chance of finding the public key value (e), then finding the decryption key (d) value directly and decrypts the cipher text, "Amare Anagaw Aycle and Vuda Sreenivasarao" **[3]** suggested an efficient representation of RSA algorithm by applying mathematical logics on two public keys rather than sending the public key (e) in RAS algorithm.. While "Gopinath Ganapathy and K Mani" **[4]** suggested a new layar of security to public key algorithm by providing more security to the cryptosystem using magic squares idea. In July 2012 Sonia Goyat**[5]** proposed a new algorithm by applying the genetic algorithm to cryptography and alter the algorithm to generate more powerful keys and also the random values, which it is used to generate keys, are unique. Then A new algorithm "Modified Subset-Sum cryptosystem over RSA" was presented by Sonal Sharma, Saroj Hiranwal, Prashant Sharma**[6]** which it is secured against Shamir attacks on RSA as well as various sorts of Mathematical attacks. And in January of the same year Prasant Sharma, Amit Kumar Gupta et al **[7]** studied the rapidity of RSA public key cryptosystem to decline the time taken for finding factor for a huge number. They suggested a new algorithm and its output was compared with "Fermats factorization Algorithm and trial division algorithm".

3. Proposed Methodology

The Improved RSA based on Double Even Magic Square (DEMS) is:-

Step 1:- Generate Doubly Even Magic Square of order 32 (32 × 32) which contains totally 1024 values and divide it to eight different quadrants each consists of 128 characters. Each different quadrant corresponds to one ASCII set (128 characters).

Step 2:- For every letter in the plain text, the numerals corresponding to its position in different quadrants of magic square are taken then these numerals are encrypted and decrypted using RSA public key cryptosystem.

Step 3:-Use the same magic square to select two prime numbers P and Q which is used to find the public key in RSA, from the range (1-1024) two numbers are selected randomly and then from this limit any two prime number (p and q) are selected which cannot be trace because of their randomness. (figure 1)

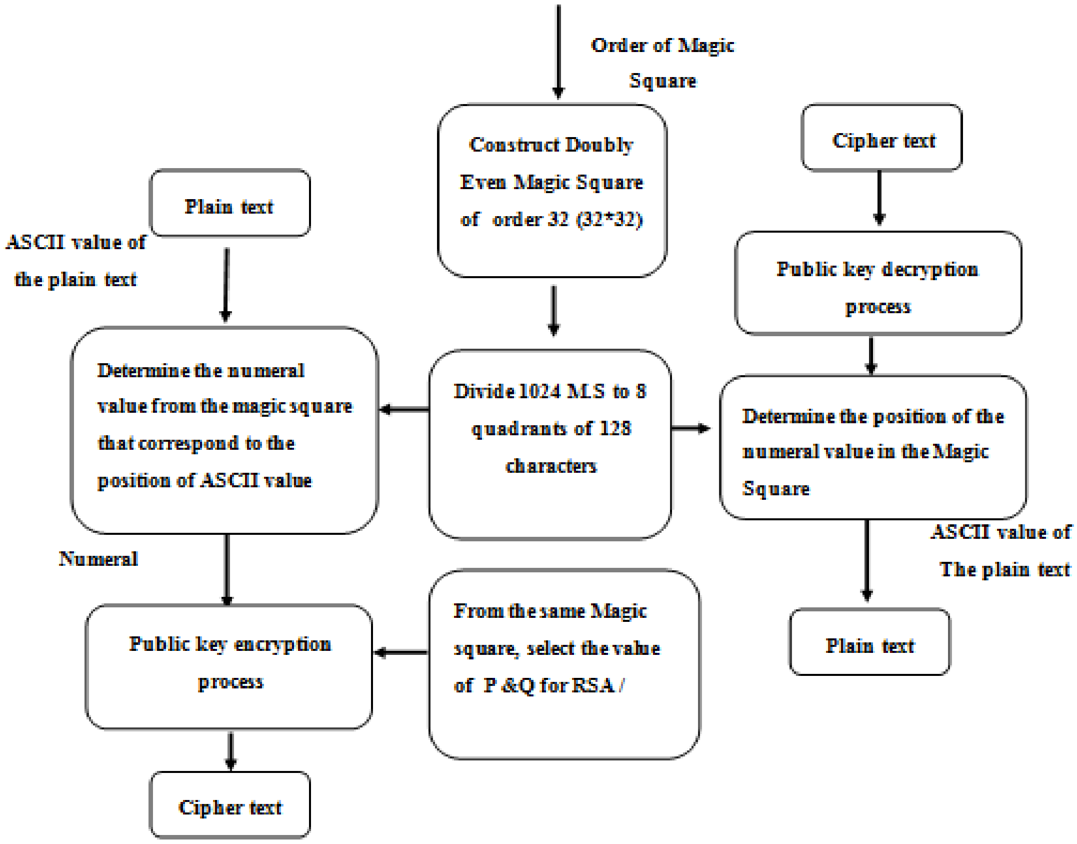

Figure 1: The Proposed Security Model

3.1. Construction of Magic Square

Kirkuk University Journal /Scientific Studies (KUJSS)
Volume 12, Issue 4, September 2017
ISSN 1992 – 0849

"A magic square" of order n is a square array or an array of n^2 numbers which fulfils the condition that the sum of the elements of each row and column, as well as the main diagonals, is the same number which it is called the magic. Generally, the entries are thought of as the natural numbers 1, 2, ..., n^2, where each number is used exactly once. Magic Squares utilized to generate a huge number of random keys. The number of magic squares of order 4 (4x4) using the numbers from 1 to 16 and magic constant (34) is 880 magic square, magic squares of order 6 (6x6) or above require a huge amount of calculations where normal computer cannot be resolved, according to some estimates the number exceeds (1.7745x1019) through rotate rows and columns. The use of magic squares in data encryption gives more security because of the difficulty of magic squares analysis using frequency analysis, Or by using the principle of guesswork and the trial and error to decode the text **[8]**. "The magic constants for normal magic squares of orders n = 3, 4, 5, 6, 7, 8 … are 15, 34, 65, 111, 175, 265… respectively".

$$Sum = n (n^2+1)/2$$

Magic squares are classified into three types: odd, doubly even and singly even **[9]**

3.2. Construction of Doubly Even Magic Squares

A doubly even magic square is a square matrix of order n, where n is divisible by four only, while a singly even magic square is a square matrix of order n, where n is even but not divisible by four. **[9]**

"A (4×4) magic square is a doubly even magic square, and one of the three types of magic square. The other two types are":

- *odd* (where n=3, 5, 7, 9, 11, etc.)

- *singly even* (even but *not* a multiple of 4 where n=6, 10, 14, 18, 22, etc.) **[4][10].**

In this paper we focused only on the implementation of doubly even magic square of order 32 (32 × 32) and their affect to enhance the public-key cryptosystem (RSA), to construct "doubly even magic squares", starting with the simplest (8×8). In 8 by 8 grids, in first step we write the numbers 1 through 64 from left to right (figure 2.a). Then "flip" the numbers in the diagonals (the red lines). That is to say, exchange 64 & 1, 55 & 10,…., and 57 & 8 and 50 & 15 and so on, and we will have a magic square constant= 260 (figure 2.b)._ in the second step we divide 8 by 8 square into 4 blocks (each block is 4 by 4) then replace and flip the elements in the secondary diagnose of block 1 with the elements in the secondary diagnose of block 4(gray cells) and replace and flip the elements in the main diagnose of block 2 with the elements in the main diagnose of block 3(yellow cells)(figure 2.c)

Kirkuk University Journal /Scientific Studies (KUJSS)
Volume 12, Issue 4, September 2017
ISSN 1992 – 0849

1	2	3	4	5	6	7	8
9	10	11	12	13	14	15	16
17	18	19	20	21	22	23	24
25	26	27	28	29	30	31	32
33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48
49	50	51	52	53	54	55	56
57	58	59	60	61	62	63	64

a

Block 1 Block 2

64	2	3	4	5	6	7	57
9	55	11	12	13	14	50	16
17	18	46	20	21	43	23	24
25	26	27	37	36	30	31	32
33	34	35	29	28	38	39	40
41	42	22	44	45	19	47	48
49	15	51	52	53	54	10	56
8	58	59	60	61	62	63	1

Block 3 Block 4

b

64	2	3	61	60	6	7	57
9	55	54	12	13	51	50	16
17	47	46	20	21	43	42	24
40	26	27	37	36	30	31	33
32	34	35	29	28	38	39	25
41	23	22	44	45	19	18	48
49	15	14	52	53	11	10	56
8	58	59	5	4	62	63	1

c

Figure 2 : Doubly Even Magic Square 8 by 8(constant 260)

With the same approach we construct a doubly even magic square of order 32 (Figure 3)

Kirkuk University Journal /Scientific Studies (KUJSS)
Volume 12, Issue 4, September 2017
ISSN 1992 – 0849

**1024 2 3 1021 1020 6 7 1017 1016 10 11 1013 1012 14 15 1009 1008 18 19 1005 1004 22 23
1001 1000 26 27 997 996 30 31 993**

**33 991 990 36 37 987 986 40 41 983 982 44 45 979 978 48 49 975 974 52 53 971 970
56 57 967 966 60 61 963 962 64**

**65 959 958 68 69 955 954 72 73 951 950 76 77 947 946 80 81 943 942 84 85 939 938
88 89 935 934 92 93 931 930 96**

**928 98 99 925 924 102 103 921 920 106 107 917 916 110 111 913 912 114 115 909 908 118 119
905 904 122 123 901 900 126 127 897**

**896 130 131 893 892 134 135 889 888 138 139 885 884 142 143 881 880 146 147 877 876 150 151
873 872 154 155 869 868 158 159 865**

**161 863 862 164 165 859 858 168 169 855 854 172 173 851 850 176 177 847 846 180 181 843 842
184 185 839 838 188 189 835 834 192**

**193 831 830 196 197 827 826 200 201 823 822 204 205 819 818 208 209 815 814 212 213 811 810
216 217 807 806 220 221 803 802 224**

**800 226 227 797 796 230 231 793 792 234 235 789 788 238 239 785 784 242 243 781 780 246 247
777 776 250 251 773 772 254 255 769**

**768 258 259 765 764 262 263 761 760 266 267 757 756 270 271 753 752 274 275 749 748 278 279
745 744 282 283 741 740 286 287 737**

**289 735 734 292 293 731 730 296 297 727 726 300 301 723 722 304 305 719 718 308 309 715 714
312 313 711 710 316 317 707 706 320**

**321 703 702 324 325 699 698 328 329 695 694 332 333 691 690 336 337 687 686 340 341 683 682
344 345 679 678 348 349 675 674 352**

**672 354 355 669 668 358 359 665 664 362 363 661 660 366 367 657 656 370 371 653 652 374 375
649 648 378 379 645 644 382 383 641**

**640 386 387 637 636 390 391 633 632 394 395 629 628 398 399 625 624 402 403 621 620 406 407
617 616 410 411 613 612 414 415 609**

**417 607 606 420 421 603 602 424 425 599 598 428 429 595 594 432 433 591 590 436 437 587 586
440 441 583 582 444 445 579 578 448**

**449 575 574 452 453 571 570 456 457 567 566 460 461 563 562 464 465 559 558 468 469 555 554
472 473 551 550 476 477 547 546 480**

**544 482 483 541 540 486 487 537 536 490 491 533 532 494 495 529 528 498 499 525 524 502 503
521 520 506 507 517 516 510 511 513**

**512 514 515 509 508 518 519 505 504 522 523 501 500 526 527 497 496 530 531 493 492 534 535
489 488 538 539 485 484 542 543 481**

**545 479 478 548 549 475 474 552 553 471 470 556 557 467 466 560 561 463 462 564 565 459 458
568 569 455 454 572 573 451 450 576**

**577 447 446 580 581 443 442 584 585 439 438 588 589 435 434 592 593 431 430 596 597 427 426
600 601 423 422 604 605 419 418 608**

**416 610 611 413 412 614 615 409 408 618 619 405 404 622 623 401 400 626 627 397 396 630 631
393 392 634 635 389 388 638 639 385**

**384 642 643 381 380 646 647 377 376 650 651 373 372 654 655 369 368 658 659 365 364 662 663
361 360 666 667 357 356 670 671 353**

Kirkuk University Journal /Scientific Studies (KUJSS)
Volume 12, Issue 4, September 2017
ISSN 1992 – 0849

673 351 350 676 677 347 346 680 681 343 342 684 685 339 338 688 689 335 334 692 693 331 330
696 697 327 326 700 701 323 322 704

705 319 318 708 709 315 314 712 713 311 310 716 717 307 306 720 721 303 302 724 725 299 298
728 729 295 294 732 733 291 290 736

288 738 739 285 284 742 743 281 280 746 747 277 276 750 751 273 272 754 755 269 268 758 759
265 264 762 763 261 260 766 767 257

256 770 771 253 252 774 775 249 248 778 779 245 244 782 783 241 240 786 787 237 236 790 791
233 232 794 795 229 228 798 799 225

801 223 222 804 805 219 218 808 809 215 214 812 813 211 210 816 817 207 206 820 821 203 202
824 825 199 198 828 829 195 194 832

833 191 190 836 837 187 186 840 841 183 182 844 845 179 178 848 849 175 174 852 853 171 170
856 857 167 166 860 861 163 162 864

160 866 867 157 156 870 871 153 152 874 875 149 148 878 879 145 144 882 883 141 140 886 887
137 136 890 891 133 132 894 895 129

128 898 899 125 124 902 903 121 120 906 907 117 116 910 911 113 112 914 915 109 108 918 919
105 104 922 923 101 100 926 927 97

929 95 94 932 933 91 90 936 937 87 86 940 941 83 82 944 945 79 78 948 949 75 74
952 953 71 70 956 957 67 66 960

961 63 62 964 965 59 58 968 969 55 54 972 973 51 50 976 977 47 46 980 981 43 42
984 985 39 38 988 989 35 34 992

32 994 995 29 28 998 999 25 24 1002 1003 21 20 1006 1007 17 16 1010 1011 13 12 1014 1015
9 8 1018 1019 5 4 1022 1023 1

Figure 3: Doubly Even Magic Square of order 32

3.2. Algorithm of generating of Doubly Even magic square:

```
Input: n is the order of doubly even magic square.

Output: Doubly Even Magic Square matrix[n][n] of order 32.

Set the array x[n][n] equal to 0
Set the array y[n][n] equal to 0
Set index to 1
For i=1 to n
        For j=1 to n
                Set tmp = ((i + 1) mod 4) / 2;
                Set x[i][j] to tmp
                Set y[i][j] to tmp
                Set Matrix[i][j]= index
                Set index to index+1
        End for j
End for i

For i=1 to n
        For j=1 to n
                If x[i][j] = y[i][j] then
                Set matrix[i][j] = n * n + 1 - matrix[i][j];
                End if
        End for j
End for i
```

4. Experiments and Results

Kirkuk University Journal /Scientific Studies (KUJSS)
Volume 12, Issue 4, September 2017
ISSN 1992 – 0849

1. Magic Square of order 4 is first generated using the proposed algorithm which satisfies the double even magic squares requirements with magic constant (34) (figure):-

16	2	3	13
5	11	10	8
9	7	6	12
4	14	15	1

Figure 3: Double even magic square of order 4

2. with the same way, we construct magic square of order 8, 16, 32 with magic constant 260, 2056, 16400 respectively (figure 4) (figure 5)(magic square of order 32 shown in figure 3) :-

64	2	3	61	60	6	7	57
9	55	54	12	13	51	50	16
17	47	46	20	21	43	42	24
40	26	27	37	36	30	31	33
32	34	35	29	28	38	39	25
41	23	22	44	45	19	18	48
56	10	11	53	52	14	15	49
8	58	59	5	4	62	63	1

Figure 4: Double even magic square of order 8

256	2	3	253	252	6	7	249	248	10	11	245	244	14	15	241
17	239	238	20	21	235	234	24	25	231	230	28	29	227	226	32
33	223	222	36	37	219	218	40	41	215	214	44	45	211	210	48
208	50	51	205	204	54	55	201	200	58	59	197	196	62	63	193
192	66	67	189	188	70	71	185	184	74	75	181	180	78	79	177
81	175	174	84	85	171	170	88	89	167	166	92	93	163	162	96
97	159	158	100	101	155	154	104	105	151	150	108	109	147	146	112
144	114	115	141	140	118	119	137	136	122	123	133	132	126	127	129
128	130	131	125	124	134	135	121	120	138	139	117	116	142	143	113
145	111	110	148	149	107	106	152	153	103	102	156	157	99	98	160
161	95	94	164	165	91	90	168	169	87	86	172	173	83	82	176
80	178	179	77	76	182	183	73	72	186	187	69	68	190	191	65
64	194	195	61	60	198	199	57	56	202	203	53	52	206	207	49
209	47	46	212	213	43	42	216	217	39	38	220	221	35	34	224
225	31	30	228	229	27	26	232	233	23	22	236	237	19	18	240
16	242	243	13	12	246	247	9	8	250	251	5	4	254	255	1

Figure 5: Double even magic square of order 16

Kirkuk University Journal /Scientific Studies (KUJSS)
Volume 12, Issue 4, September 2017
ISSN 1992 – 0849

It is so difficult to determine the number of unique magic squares of different orders, but the number of unique magic squares of order n=1, 2, ... are 1, 0, 1, 880, 275305224 . The 880 squares of order 4 were enumerated by "Frénicle de Bessy" in 1693, and are illustrated in Berlekamp (1982). "R. Schroeppel" in 1973 calculate the number of (5×5) magic squares[13], while the number of (6×6) squares is not identified, but "Pinn and Wieczerkowski (1998)" estimated it to be (1.7745(16)×1019) [14].

5. Example on RSA with double even Magic Square

RSA is implemented to illustrate the effect of using magic squares to enhance the security of public key encryption schemes. The secret key in the system consists of two prime numbers (P and Q) and an exponent (d) while the public key consists of the modulus N = P.Q and an exponent (e) where $d = e^{-1}$ mod (P-1) (Q-1). The user calculates $C = M^e$ mod (n) for encryption and $M = C^d$ mod (n) is done for decryption (for any message [11],[12].

In this paper, the modulus of N, M, and C should have a length of 512-1024 bits in order to prevent the known attacks. Using the above algorithm, we construct a " doubly even magic square" of order 32 which contains 1024 different (non repetition) values, as the characters set consists of 128 ASCII values, the magic square is divided logically into different 8 matrices each one with 128 values corresponding to individual ASCII character, for getting more realization of the proposed matter, we take an example, assume P=13, Q=17 and the public key (e) =11, then N=221, and (P-1).(Q-1)=192 .now the secret key(d) = 35 . To encrypt the message (A CAR), the ASCII values of A, C and R are 65, 67 and 82 respectively, so to encrypt A which appears in first and third position in the plain text, the numerals which appear at 65th position of first matrices and at 65th position of third matrices(figure 3 which is divided logically into 8 matrice) are taken respectively, Thus $N_p(A)=959$ and 831, $N_p(C)=68$ and $N_p(R)$ =942. And the cipher $C(A)=959^{11}$ mod 221=82, $C(C)=68^{11}$ mod 221=204, $C(A)=831^{11}$ mod 221=77, $C(R)=942^{11}$ mod 221=167 similarly we use this

Kirkuk University Journal /Scientific Studies (KUJSS)
Volume 12, Issue 4, September 2017
ISSN 1992 – 0849

substitution for every repeated character in the plaintext, therefore for each repeated character A, B, C,....(which appears more than once in the plain text), different cipher texts are generated.

6. The comparison between ordinary RSA algorithm and proposed RSA with Double Even Magic Square:-

To illustrate the result of RSA algorithm with magic square, the plain text (MESSAGE) is first encrypted using existing RSA(if p=19, q=23, n=437, (p-1).(q-1)=396, e=13 then d=61) and the output is shown in table 1. It is clear that the characters (E and S) appear twice in the plaintext, therefore in the ordinary RSA, the cipher text of them is the same (425), while in the suggested (RSA with DEMS), the cipher text value of the first (E) which it is (397) is differ from the second (E) which it is (298) and the same thing with any repeated characters in the plaintext, This methodology is implemented in C#

Table 1. Comparison of cipher text

Ordinary RSA			RSA with Double even magic square		
Plain text	ASCII value	Cipher text	Plain text	MS value	Cipher text
M	77	248	M	947	62
E	69	69	E	955	397
S	83	425	S	84	350
S	83	425	S	212	90
A	65	122	A	959	348
G	71	211	G	72	124
E	69	69	E	827	298

7. Conclusion

This work prevents any hacker from getting the plain text in a readable form even if they obtained the keys because of using the numerical values of magic square rather than the ASCII values of characters (rather than of unique ASCII table, 8 tables with various set of values are used). It is unsolved problem to determine the number of magic squares of order 32 which is used in this paper. The security aspect of RSA is improved because there are no duplicated values in Magic Squares. In the ordinary RSA, the same cipher text values are generated whenever the same characters are repeated in the plain text, while in the proposed (RSA with DEMS) different values are produced in the cipher text for each occurrence of the same character in the plain text. It plays an important role in increasing the randomness and security of the algorithm. One of the issues in the proposed work is additional time needed for the construction of Magic squares initially.

REFERENCES

[1] Andrew Zwicke, " An Introduction to Modren Cryptosystems", GIAC Institute version 1.4b, option1, 2003.

[2] A. J. Menezes, P.C. Van Oorschot, and S. Vanstone, "*Handbook of Applied Cryptography",* CRC Press, Boca Ration, Florida, USA, 1997.

[3] Amare Anagaw Ayele1 , Dr. Vuda Sreenivasarao.," A Modified RSA Encryption Technique Based on Multiple public keys, International Journal of Innovative Research in Computer and Communication Engineering ISSN (Online): 2320 – 9801Vol.1, Issue 4, June 2013

[4] Gopinath Ganapathy, and K.Mani , " Add-On Security Model for public key Cryptosystem Based on Magic Square Implementation", ISBN 978-988-17012-6-8, Proceedings of the world congress on Engineering and Computer Science 2009 Vol I, San Fransisco, USA.

[5] Sonia Goyat.," Genetic key generation for public key cryptography ",International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-2, Issue-3, July 2012.

[6] Sonal Sharma, Saroj Hiranwal, Prashant Sharma A new variant of subset-sum cryptosystem over RSA, International Journal of Advances in Engineering & Technology, Jan 2012.©IJAET ISSN: 2231-1963.

[7] Sharma, P. Gupta, A.K. ; Vijay, A. "Modified Integer Factorization Algorithm Using V-Factor Method" Page(s): 423 - 425 ,978-0-7695-4640-7/12, IEEE 2012.

[8] K. Pinn and C. Wieczerkowski, Number of Magic Squares From Parallel Tempering Monte Carlo, ar Xiv:cond-mat/984109v1, Germany, 9 Apr. 1998.

[9] http://en.wikipedia.org/wiki/Magic_ squares , pp. 1-3.

[10] Adam Rogers, and Peter Loly ,"The inertial properties of Squares and Cubes", Nov-2004, pp.1-3.

[11] B.Schneier, "Applied Cryptography", John Wiley & Sons Inc., New York, Second Edition, 1996.

[12] Stallings,"Cryptography and Network Security", Prentice Hall, Upper

Saddle River, New Jersey, USA, Second Edition, 1997.

[13] I. Cameron, A. Rogers and P.Loly, "The Library of Magical Squares" Department of Physics and Astronomy, University of Manitoba, Winnipeg, Manitoba, Canada R3T 2N2, 19 July 2012

[14] Trump, W. 2003 Estimate of the number of magic squares of order 6. http://www.trump.de/magic-squares/normal-6/index.html.