Dicle University Journal of Engineering (DUJE)

web: http://dergipark.gov.tr/dumf

Research Article

Matrix Encryption Standard

Orhan Dişkaya*[1] , Erdinç Avaroğlu[2] and Hamza Menken[3]

1 Mersin University, Graduate School of Natural and Applied Sciences, Ciftlikkoy, Mersin, TURKEY, orhandiskaya@mersin.edu.tr, ORCID ID 0000-0001-5698-7834

2 Mersin University, Computer Engineering Department, Ciftlikkoy, Mersin, TURKEY, eavaroglu@mersin.edu.tr, ORCID ID 0000-0003-1976-2526

3 Mersin University, Department of Mathematics Ciftlikkoy, Mersin, TURKEY, hmenken@mersin.edu.tr, ORCID ID 0000-0003-1194-3162

ARTICLE INFO

Article history:

Received 7 May 2020
Received in revised form 10 July 2020
Accepted 18 August 2020
Available online 30 September 2020

Keywords:

Cryptology, Encryption, AES, Matrix

Doi: 10.24012/dumf.733498

ABSTRACT

AES (Advanced Encryption Standard) is a standard for encrypting electronic data. AES operates on a 4×4 column-major order array of bytes. The operations in the matrix are also performed on the polynomials in a special finite field and using S-box. We firstly recall necessary information about matrix algebra. In the present work, we examine the AES encryption method. We create a new encryption algorithm called matrix encryption standard (MES). MES is performed by similar steps to the AES algorithm over 16x16 matrices with elements {0,1} without using polynomials operations and S-box in the AES algorithm. So, we provide 256-bits plain text to be encrypted by passing it through certain rounds with the 16x16 matrix key. In order to decrypt the cipher text, we take the reverse of the 16x16 key matrix through the computer and perform the decryption process by performing a certain number of reverse rounds.

* Corresponding author
Orhan, Dişkaya
✉ , orhandiskaya@mersin.edu.tr

Please cite this article in press as O. Diskaya, E. Avaroglu, H. Menken, "Matrix Encryption Standard", DUJE, vol. 11, no.3, pp. 999-1010, September 2020.

Introduction

Cryptology is password science. It is the encryption of various messages, texts according to a certain system, these messages are transmitted to the receiver in a secure environment and the transmitted message is deciphered. Cryptology science is divided into two branches. These are Cryptography; encrypted writing and Cryptanalysis; deciphering or analyzing passwords. Cryptology has a very ancient history. These are Caesar encryption, rotor machine (Enigma), public-key encryption, data hiding techniques. Cryptology algorithms consist entirely of mathematical functions. One of the most important encryption algorithms that include mathematical functions is AES (Advanced Encryption Standard). AES is a standard for encrypting electronic data. AES adopted by the American government is also used as defacto encryption (crypto) standard internationally. It has replaced DES (Data Encryption Standard). It is a symmetric-switched algorithm. The encryption and decryption keys are the same for AES. It is based on the design basis known as Substitution-Permutation. Its software and hardware performance is high. It runs on a 4x4 matrix called state. The operations on the matrix are made in a special finite field. The algorithm consists of a number of repetitive input clear texts, round identical conversion cycles that convert the output into encrypted text. Each cycle consists of four steps, except for the last cycle. These cycles are applied in reverse order to decode the encrypted text. The repeat numbers of the cycles are 10, 12, and 14, respectively, for key lengths of 128-bit, 192-bit, and 256-bit. The round transformation is composed of four different transformations. These are byte sub, shift row, mix column and add round key. The final round of the cipher is slightly different. It is defined by byte sub, shift row and add round key. In this study, we create a new encryption algorithm called matrix encryption standard (MES) with AES similar properties. MES has 256-bit keys and works with around conversion process like AES. These processes are transpose, shift column, inverse reflection and add round key, respectively. So, we first express some of the properties of the matrix that form the basis of the MES encryption algorithm. For more information on cryptology, see [3,4,5,6].

Matrices were jointly discovered by Arthur Cayley and James Joseph Sylvester. A matrix is a rectangular configuration of the numbers in square brackets. P matrix with m rows and n columns is an $m\times n$ matrix, its size being $m\times n$. When m is 1, it is a row vector; and when n is 1, it is a column vector. If $m=n$, it is a square matrix of order n. Every number in the arrangement is an element of the matrix. Let p_{ij} show the element in column j and row i of P. Then, matrix has the following form,

$$P=\begin{pmatrix} p_{11} & \cdots & p_{1n} \\ \vdots & \ddots & \vdots \\ p_{m1} & \cdots & p_{mn} \end{pmatrix} \quad (1)$$

When all elements of the matrix are zero, this matrix is zero matrix, denoted by O_n. For example,

$$O_2=\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \text{ and } O_3=\begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \quad (2)$$

The identity matrix of order n is denoted by I_n. For example,

$$I_2=\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \text{ and } I_3=\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad (3)$$

For each square matrix $P=\left(p_{ij}\right)$, define transpose P, denoted by P^T, that is

$$P=\begin{pmatrix} p_{11} & \cdots & p_{1n} \\ \vdots & \ddots & \vdots \\ p_{n1} & \cdots & p_{nn} \end{pmatrix} \text{ then, } P^T=\begin{pmatrix} p_{11} & \cdots & p_{m1} \\ \vdots & \ddots & \vdots \\ p_{1n} & \cdots & p_{nn} \end{pmatrix} \quad (4)$$

The sum of the matrices $P=\left(p_{ij}\right)_{m\times n}$ and $Q=\left(q_{ij}\right)_{m\times n}$ is defined by $P+Q=\left(p_{ij}+q_{ij}\right)_{m\times n}$, that is

$$P+Q=\begin{pmatrix} p_{11}+q_{11} & \cdots & p_{1n}+q_{1n} \\ \vdots & \ddots & \vdots \\ p_{m1}+q_{m1} & \cdots & p_{mn}+q_{mn} \end{pmatrix} \quad (5)$$

Let $P=\left(p_{ij}\right)$ be any matrix and k any real number. Then, $kP=\left(kp_{ij}\right)_{m\times n}$, that is

$$kP=\begin{pmatrix} kp_{11} & \cdots & kp_{1n} \\ \vdots & \ddots & \vdots \\ kp_{m1} & \cdots & kp_{mn} \end{pmatrix} \quad (6)$$

The product PQ of the matrices $P=\left(p_{ij}\right)_{m\times n}$ and $Q=\left(q_{ij}\right)_{m\times n}$ is the matrix $R=\left(r_{ij}\right)_{m\times n}$ where r_{ij} is the sum of the products of the corresponding elements in column j of Q and row i of P, as shown below:

$$\begin{pmatrix} p_{11} & \cdots & p_{1n} \\ \vdots & \ddots & \vdots \\ p_{m1} & \cdots & p_{mn} \end{pmatrix}\begin{pmatrix} q_{11} & \cdots & q_{1n} \\ \vdots & \ddots & \vdots \\ q_{m1} & \cdots & q_{mn} \end{pmatrix}=\begin{pmatrix} \ddots & \vdots & \iddots \\ \cdots & r_{ij} & \cdots \\ \iddots & \vdots & \ddots \end{pmatrix} \quad (7)$$

where $r_{ij}=p_{i1}q_{1j}+p_{i2}q_{2j}+\cdots+p_{in}q_{nj}=\sum_{k=1}^{n}p_{ik}q_{kj}$.

For each basic transformation, there is an inverse transformation, that is, a transformation that undoes everything that the basic transformation does. The inverse of the matrix can be taken in several ways. These are Gauss-Jordan method, inverse of a matrix using minors, cofactors and ad-jugate and programs for the inverse of large matrices. More information about the matrix can be viewed at [2].

ASCII Table

It is one of the tables used in computer science and used to express each symbol numerically. ASCII letters consist of the initials of the words American Standard Code for Information Interchange. It is simply used to translate the signals processed by the computer (which can be shown as 1 and 0) into symbols that people can understand. The encryption of the algorithm puts forward in this study is carried out using the table.

Table 1. Ascıı table

Dec	Hex	Oct	Char	Dec	Hex	Oct	Char	Dec	Hex	Oct	Char	Dec	Hex	Oct	Char
0	0	0		32	20	40	[space]	64	40	100	@	96	60	140	`
1	1	1		33	21	41	!	65	41	101	A	97	61	141	A
2	2	2		34	22	42	“	66	42	102	B	98	62	142	B
3	3	3		35	23	43	#	67	43	103	C	99	63	143	C
4	4	4		36	24	44	$	68	44	104	D	100	64	144	D
5	5	5		37	25	45	%	69	45	105	E	101	65	145	E
6	6	6		38	26	46	&	70	46	106	F	102	66	146	F
7	7	7		39	27	47	‘	71	47	107	G	103	67	147	G
8	8	10		40	28	50	(	72	48	110	H	104	68	150	H
9	9	11		41	29	51	)	73	49	111	I	105	69	151	I
10	A	12		42	2A	52	*	74	4A	112	J	106	6A	152	J
11	B	13		43	2B	53	+	75	4B	113	K	107	6B	153	K
12	C	14		44	2C	54	,	76	4C	114	L	108	6C	154	L
13	D	15		45	2D	55	-	77	4D	115	M	109	6D	155	M
14	E	16		46	2E	56	.	78	4E	116	N	110	6E	156	N
15	F	17		47	2F	57	/	79	4F	117	O	111	6F	157	O
16	10	20		48	30	60	0	80	50	120	P	112	70	160	P
17	11	21		49	31	61	1	81	51	121	Q	113	71	161	Q
18	12	22		50	32	62	2	82	52	122	R	114	72	162	R
19	13	23		51	33	63	3	83	53	123	S	115	73	163	S
20	14	24		52	34	64	4	84	54	124	T	116	74	164	T
21	15	25		53	35	65	5	85	55	125	U	117	75	165	U
22	16	26		54	36	66	6	86	56	126	V	118	76	166	V
23	17	27		55	37	67	7	87	57	127	W	119	77	167	W
24	18	30		56	38	70	8	88	58	130	X	120	78	170	X
25	19	31		57	39	71	9	89	59	131	Y	121	79	171	Y
26	1A	32		58	3A	72	:	90	5A	132	Z	122	7A	172	Z
27	1B	33		59	3B	73	;	91	5B	133	[	123	7B	173	{
28	1C	34		60	3C	74	<	92	5C	134	\	124	7C	174	|
29	1D	35		61	3D	75	=	93	5D	135	]	125	7D	175	}
30	1E	36		62	3E	76	>	94	5E	136	^	126	7E	176	
31	1F	37		63	3F	77	?	95	5F	137	-	127	7F	177	

Main Results

In the section, we aim to create a new encryption algorithm without using the polynomials in the AES. We consider as a row vector matrix of type

$$\left[\lambda_{i(4j-3)}\lambda_{i(4j-2)}\lambda_{i(4j-1)}\lambda_{i(4j)}\right]_{1\times 4}, \left\{\lambda_{ij}\in\{0,1\}\,\middle|\, i,j\in\square^{+}\right\} \quad (8)$$

as 4 bits and find the corresponding value with the result $2^3\lambda_{i(4j-3)}+2^2\lambda_{i(4j-2)}+2^1\lambda_{i(4j-1)}+2^0\lambda_{i(4j)}$

and the equivalent of this result appears in the ASCII table.

Table 2. Hexadecimal equivalent of the binary

$[0000]=0$	$[0100]=4$	$[1000]=8$	$[1100]=C$
$[0001]=1$	$[0101]=5$	$[1001]=9$	$[1101]=D$
$[0010]=2$	$[0110]=6$	$[1010]=A$	$[1110]=E$
$[0011]=3$	$[0111]=7$	$[1011]=B$	$[1111]=F$

So that, the values of the A, B, C, D, E, F in Table 2 are known to be 10, 11, 12, 13, 14, 15, respectively.

The 16×16 matrix is obtained by placing a 4-bit row matrix for each value of the 4×16 status matrix. For example, let's show the hexadecimal state matrix as a binary 16×16 matrix on the example as below

Table 3. State matrix

$$\begin{pmatrix} 2 & 1 & A & C \\ B & 3 & 0 & D \\ 5 & 4 & 9 & F \\ 7 & E & 6 & 8 \\ \vdots & \vdots & \vdots & \vdots \end{pmatrix} = \begin{pmatrix} 0&0&1&0&0&0&0&1&1&0&1&0&1&1&0&0 \\ 1&0&1&1&0&0&1&1&0&0&0&0&1&1&0&1 \\ 0&1&0&1&0&1&0&0&1&0&0&1&1&1&1&1 \\ 0&1&1&1&1&1&1&0&0&1&1&0&1&0&0&0 \\ \vdots&\vdots&\vdots&\vdots&\vdots&\vdots&\vdots&\vdots&\vdots&\vdots&\vdots&\vdots&\vdots&\vdots&\vdots&\vdots \end{pmatrix}_{16\times16}$$

So, the input 256-bits is organized as a 16×16 matrix of cells, where each cell is one bit.

Table 4. State matrix

$$\begin{pmatrix} x_{11} & x_{12} & x_{13} & x_{14} & x_{15} & x_{16} & x_{17} & x_{18} & x_{19} & x_{1A} & x_{1B} & x_{1C} & x_{1D} & x_{1E} & x_{1F} & x_{1G} \\ x_{21} & x_{22} & x_{23} & x_{24} & x_{25} & x_{26} & x_{27} & x_{28} & x_{29} & x_{2A} & x_{2B} & x_{2C} & x_{2D} & x_{2E} & x_{2F} & x_{2G} \\ x_{31} & x_{32} & x_{33} & x_{34} & x_{35} & x_{36} & x_{37} & x_{38} & x_{39} & x_{3A} & x_{3B} & x_{3C} & x_{3D} & x_{3E} & x_{3F} & x_{3G} \\ x_{41} & x_{42} & x_{43} & x_{44} & x_{45} & x_{46} & x_{47} & x_{48} & x_{49} & x_{4A} & x_{4B} & x_{4C} & x_{4D} & x_{4E} & x_{4F} & x_{4G} \\ x_{51} & x_{52} & x_{53} & x_{54} & x_{55} & x_{56} & x_{57} & x_{58} & x_{59} & x_{5A} & x_{5B} & x_{5C} & x_{5D} & x_{5E} & x_{5F} & x_{5G} \\ x_{61} & x_{62} & x_{63} & x_{64} & x_{65} & x_{66} & x_{67} & x_{68} & x_{69} & x_{6A} & x_{6B} & x_{6C} & x_{6D} & x_{6E} & x_{6F} & x_{6G} \\ x_{71} & x_{72} & x_{73} & x_{74} & x_{75} & x_{76} & x_{77} & x_{78} & x_{79} & x_{7A} & x_{7B} & x_{7C} & x_{7D} & x_{7E} & x_{7F} & x_{7G} \\ x_{81} & x_{82} & x_{83} & x_{84} & x_{85} & x_{86} & x_{87} & x_{88} & x_{89} & x_{8A} & x_{8B} & x_{8C} & x_{8D} & x_{8E} & x_{8F} & x_{8G} \\ x_{91} & x_{92} & x_{93} & x_{94} & x_{95} & x_{96} & x_{97} & x_{98} & x_{99} & x_{9A} & x_{9B} & x_{9C} & x_{9D} & x_{9E} & x_{9F} & x_{9G} \\ x_{A1} & x_{A2} & x_{A3} & x_{A4} & x_{A5} & x_{A6} & x_{A7} & x_{A8} & x_{A9} & x_{AA} & x_{AB} & x_{AC} & x_{AD} & x_{AE} & x_{AF} & x_{AG} \\ x_{B1} & x_{B2} & x_{B3} & x_{B4} & x_{B5} & x_{B6} & x_{B7} & x_{B8} & x_{B9} & x_{BA} & x_{BB} & x_{BC} & x_{BD} & x_{BE} & x_{BF} & x_{BG} \\ x_{C1} & x_{C2} & x_{C3} & x_{C4} & x_{C5} & x_{C6} & x_{C7} & x_{C8} & x_{C9} & x_{CA} & x_{CB} & x_{CC} & x_{CD} & x_{CE} & x_{CF} & x_{CG} \\ x_{D1} & x_{D2} & x_{D3} & x_{D4} & x_{D5} & x_{D6} & x_{D7} & x_{D8} & x_{D9} & x_{DA} & x_{DB} & x_{DC} & x_{DD} & x_{DE} & x_{DF} & x_{DG} \\ x_{E1} & x_{E2} & x_{E3} & x_{E4} & x_{E5} & x_{E6} & x_{E7} & x_{E8} & x_{E9} & x_{EA} & x_{EB} & x_{EC} & x_{ED} & x_{EE} & x_{EF} & x_{EG} \\ x_{F1} & x_{F2} & x_{F3} & x_{F4} & x_{F5} & x_{F6} & x_{F7} & x_{F8} & x_{F9} & x_{FA} & x_{FB} & x_{FC} & x_{FD} & x_{FE} & x_{FF} & x_{FG} \\ x_{G1} & x_{G2} & x_{G3} & x_{G4} & x_{G5} & x_{G6} & x_{G7} & x_{G8} & x_{G9} & x_{GA} & x_{GB} & x_{GC} & x_{GD} & x_{GE} & x_{GF} & x_{GG} \end{pmatrix}_{16\times16}$$

The MES algorithm

As with most block cipher algorithms, the number of cycles of the MES varies depending on the size of the secret key. The number of cycles in AES is indicated in parentheses in Table 5.

Table 5. Number of rounds

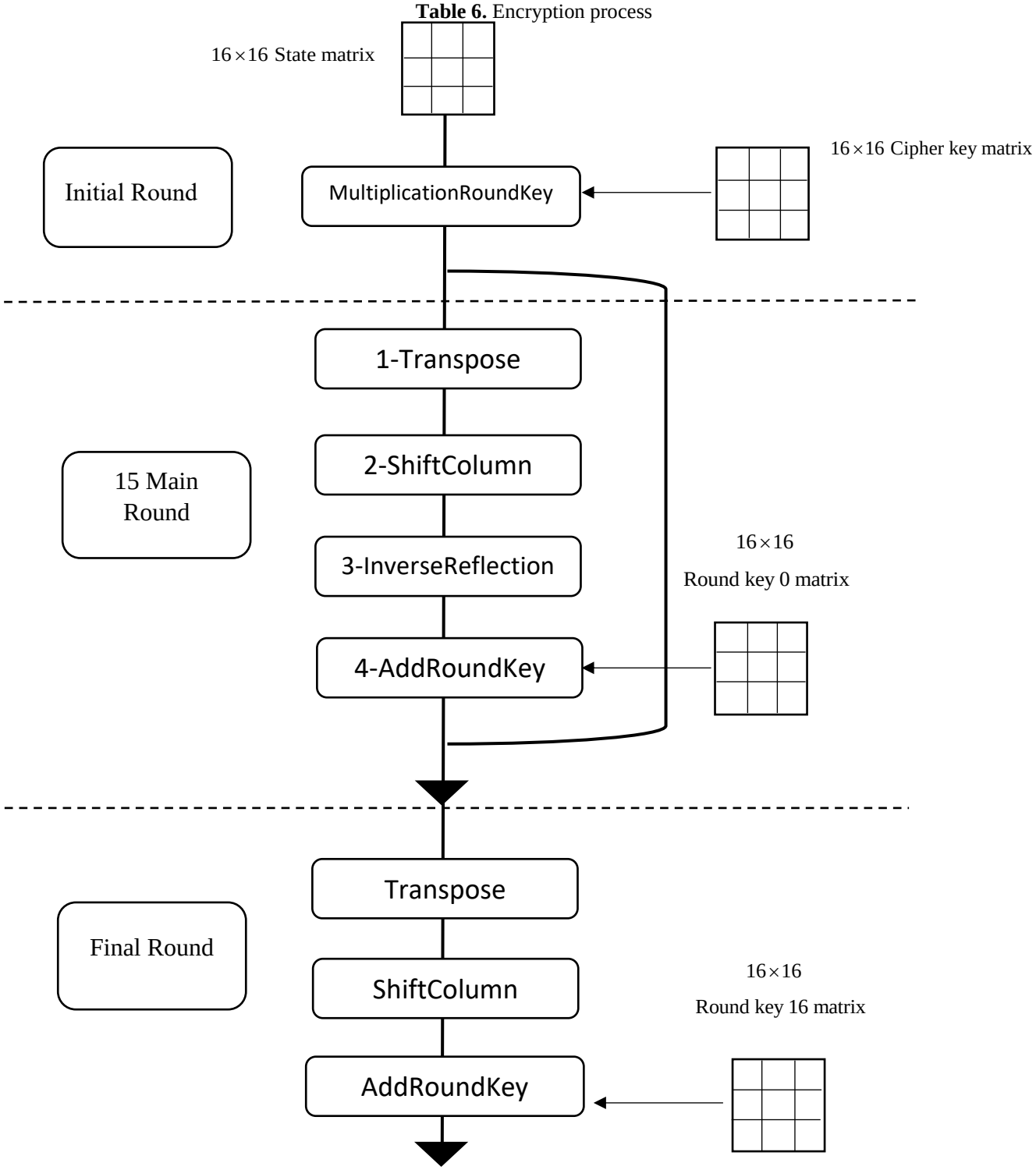
Cipher name	Key-size(bits)	Number of rounds
MES-64 (AES-128)	64 (128)	8 (10)
MES-256 (AES-192)	256 (192)	16 (12)
MES-1028 (AES-256)	1028 (256)	32 (14)

AES studies in [1,3,4,5,6] can be examined to understand better the MES algorithm.

The MES Encryption Process

Here, we create a description of a typical round of the MES encryption process. It takes place in three stages. In the first stage, the multiplication of the state matrix and the cipher key matrix occur. In the second stage, each round consists of the four processes conducted in the order. So, transpose, shift column, inverse reflection and add round key operate 15 times, respectively. In the last stage, the final state matrix adds with the round key 16 matrix after taking its transpose and shift column, respectively, and the text is encrypted.

Table 6. Encryption process



Cipher key: Let's firstly determine a random 16×16 cipher key matrix in Table 7.

Table 7. Cipher key matrix

$$\begin{pmatrix}
y_{11} & y_{12} & y_{13} & y_{14} & y_{15} & y_{16} & y_{17} & y_{18} & y_{19} & y_{1A} & y_{1B} & y_{1C} & y_{1D} & y_{1E} & y_{1F} & y_{1G} \\
y_{21} & y_{22} & y_{23} & y_{24} & y_{25} & y_{26} & y_{27} & y_{28} & y_{29} & y_{2A} & y_{2B} & y_{2C} & y_{2D} & y_{2E} & y_{2F} & y_{2G} \\
y_{31} & y_{32} & y_{33} & y_{34} & y_{35} & y_{36} & y_{37} & y_{38} & y_{39} & y_{3A} & y_{3B} & y_{3C} & y_{3D} & y_{3E} & y_{3F} & y_{3G} \\
y_{41} & y_{42} & y_{43} & y_{44} & y_{45} & y_{46} & y_{47} & y_{48} & y_{49} & y_{4A} & y_{4B} & y_{4C} & y_{4D} & y_{4E} & y_{4F} & y_{4G} \\
y_{51} & y_{52} & y_{53} & y_{54} & y_{55} & y_{56} & y_{57} & y_{58} & y_{59} & y_{5A} & y_{5B} & y_{5C} & y_{5D} & y_{5E} & y_{5F} & y_{5G} \\
y_{61} & y_{62} & y_{63} & y_{64} & y_{65} & y_{66} & y_{67} & y_{68} & y_{69} & y_{6A} & y_{6B} & y_{6C} & y_{6D} & y_{6E} & y_{6F} & y_{6G} \\
y_{71} & y_{72} & y_{73} & y_{74} & y_{75} & y_{76} & y_{77} & y_{78} & y_{79} & y_{7A} & y_{7B} & y_{7C} & y_{7D} & y_{7E} & y_{7F} & y_{7G} \\
y_{81} & y_{82} & y_{83} & y_{84} & y_{85} & y_{86} & y_{87} & y_{88} & y_{89} & y_{8A} & y_{8B} & y_{8C} & y_{8D} & y_{8E} & y_{8F} & y_{8G} \\
y_{91} & y_{92} & y_{93} & y_{94} & y_{95} & y_{96} & y_{97} & y_{98} & y_{99} & y_{9A} & y_{9B} & y_{9C} & y_{9D} & y_{9E} & y_{9F} & y_{9G} \\
y_{A1} & y_{A2} & y_{A3} & y_{A4} & y_{A5} & y_{A6} & y_{A7} & y_{A8} & y_{A9} & y_{AA} & y_{AB} & y_{AC} & y_{AD} & y_{AE} & y_{AF} & y_{AG} \\
y_{B1} & y_{B2} & y_{B3} & y_{B4} & y_{B5} & y_{B6} & y_{B7} & y_{B8} & y_{B9} & y_{BA} & y_{BB} & y_{BC} & y_{BD} & y_{BE} & y_{BF} & y_{BG} \\
y_{C1} & y_{C2} & y_{C3} & y_{C4} & y_{C5} & y_{C6} & y_{C7} & y_{C8} & y_{C9} & y_{CA} & y_{CB} & y_{CC} & y_{CD} & y_{CE} & y_{CF} & y_{CG} \\
y_{D1} & y_{D2} & y_{D3} & y_{D4} & y_{D5} & y_{D6} & y_{D7} & y_{D8} & y_{D9} & y_{DA} & y_{DB} & y_{DC} & y_{DD} & y_{DE} & y_{DF} & y_{DG} \\
y_{E1} & y_{E2} & y_{E3} & y_{E4} & y_{E5} & y_{E6} & y_{E7} & y_{E8} & y_{E9} & y_{EA} & y_{EB} & y_{EC} & y_{ED} & y_{EE} & y_{EF} & y_{EG} \\
y_{F1} & y_{F2} & y_{F3} & y_{F4} & y_{F5} & y_{F6} & y_{F7} & y_{F8} & y_{F9} & y_{FA} & y_{FB} & y_{FC} & y_{FD} & y_{FE} & y_{FF} & y_{FG} \\
y_{G1} & y_{G2} & y_{G3} & y_{G4} & y_{G5} & y_{G6} & y_{G7} & y_{G8} & y_{G9} & y_{GA} & y_{GB} & y_{GC} & y_{GD} & y_{GE} & y_{GF} & y_{GG}
\end{pmatrix}_{16\times16}$$

Elements of the above matrix are determined by the set $\left\{x_{ij}\in\{0,1\}\middle| i,j\in\square^{+}\right\}$.

Multiplication round key: In this step, the state matrix and cipher key are performed multiplication with each other. It is obtained the matrix in Table 8.

Table 8. Multiplication matrix

$$\begin{pmatrix}
z_{11} & z_{12} & z_{13} & z_{14} & z_{15} & z_{16} & z_{17} & z_{18} & z_{19} & z_{1A} & z_{1B} & z_{1C} & z_{1D} & z_{1E} & z_{1F} & z_{1G} \\
z_{21} & z_{22} & z_{23} & z_{24} & z_{25} & z_{26} & z_{27} & z_{28} & z_{29} & z_{2A} & z_{2B} & z_{2C} & z_{2D} & z_{2E} & z_{2F} & z_{2G} \\
z_{31} & z_{32} & z_{33} & z_{34} & z_{35} & z_{36} & z_{37} & z_{38} & z_{39} & z_{3A} & z_{3B} & z_{3C} & z_{3D} & z_{3E} & z_{3F} & z_{3G} \\
z_{41} & z_{42} & z_{43} & z_{44} & z_{45} & z_{46} & z_{47} & z_{48} & z_{49} & z_{4A} & z_{4B} & z_{4C} & z_{4D} & z_{4E} & z_{4F} & z_{4G} \\
z_{51} & z_{52} & z_{53} & z_{54} & z_{55} & z_{56} & z_{57} & z_{58} & z_{59} & z_{5A} & z_{5B} & z_{5C} & z_{5D} & z_{5E} & z_{5F} & z_{5G} \\
z_{61} & z_{62} & z_{63} & z_{64} & z_{65} & z_{66} & z_{67} & z_{68} & z_{69} & z_{6A} & z_{6B} & z_{6C} & z_{6D} & z_{6E} & z_{6F} & z_{6G} \\
z_{71} & z_{72} & z_{73} & z_{74} & z_{75} & z_{76} & z_{77} & z_{78} & z_{79} & z_{7A} & z_{7B} & z_{7C} & z_{7D} & z_{7E} & z_{7F} & z_{7G} \\
z_{81} & z_{82} & z_{83} & z_{84} & z_{85} & z_{86} & z_{87} & z_{88} & z_{89} & z_{8A} & z_{8B} & z_{8C} & z_{8D} & z_{8E} & z_{8F} & z_{8G} \\
z_{91} & z_{92} & z_{93} & z_{94} & z_{95} & z_{96} & z_{97} & z_{98} & z_{99} & z_{9A} & z_{9B} & z_{9C} & z_{9D} & z_{9E} & z_{9F} & z_{9G} \\
z_{A1} & z_{A2} & z_{A3} & z_{A4} & z_{A5} & z_{A6} & z_{A7} & z_{A8} & z_{A9} & z_{AA} & z_{AB} & z_{AC} & z_{AD} & z_{AE} & z_{AF} & z_{AG} \\
z_{B1} & z_{B2} & z_{B3} & z_{B4} & z_{B5} & z_{B6} & z_{B7} & z_{B8} & z_{B9} & z_{BA} & z_{BB} & z_{BC} & z_{BD} & z_{BE} & z_{BF} & z_{BG} \\
z_{C1} & z_{C2} & z_{C3} & z_{C4} & z_{C5} & z_{C6} & z_{C7} & z_{C8} & z_{C9} & z_{CA} & z_{CB} & z_{CC} & z_{CD} & z_{CE} & z_{CF} & z_{CG} \\
z_{D1} & z_{D2} & z_{D3} & z_{D4} & z_{D5} & z_{D6} & z_{D7} & z_{D8} & z_{D9} & z_{DA} & z_{DB} & z_{DC} & z_{DD} & z_{DE} & z_{DF} & z_{DG} \\
z_{E1} & z_{E2} & z_{E3} & z_{E4} & z_{E5} & z_{E6} & z_{E7} & z_{E8} & z_{E9} & z_{EA} & z_{EB} & z_{EC} & z_{ED} & z_{EE} & z_{EF} & z_{EG} \\
z_{F1} & z_{F2} & z_{F3} & z_{F4} & z_{F5} & z_{F6} & z_{F7} & z_{F8} & z_{F9} & z_{FA} & z_{FB} & z_{FC} & z_{FD} & z_{FE} & z_{FF} & z_{FG} \\
z_{G1} & z_{G2} & z_{G3} & z_{G4} & z_{G5} & z_{G6} & z_{G7} & z_{G8} & z_{G9} & z_{GA} & z_{GB} & z_{GC} & z_{GD} & z_{GE} & z_{GF} & z_{GG}
\end{pmatrix}_{16\times16}$$

$$z_{ij} = x_{i1}y_{1j} + x_{i2}y_{2j} + \cdots + x_{in}y_{nj} = \sum_{k=1}^{G} x_{ik}y_{kj} \pmod 2 \quad (9)$$

Transpose: This step performs the transposition of 16×16 matrix. This transformation is shown in Table 9.

Table 9. Transpose matrix

$$\begin{pmatrix}
z_{11} & z_{21} & z_{31} & z_{41} & z_{51} & z_{61} & z_{71} & z_{81} & z_{91} & z_{A1} & z_{B1} & z_{C1} & z_{D1} & z_{E1} & z_{F1} & z_{G1} \\
z_{12} & z_{22} & z_{32} & z_{42} & z_{52} & z_{62} & z_{72} & z_{82} & z_{92} & z_{A2} & z_{B2} & z_{C2} & z_{D2} & z_{E2} & z_{F2} & z_{G2} \\
z_{13} & z_{23} & z_{33} & z_{43} & z_{53} & z_{63} & z_{73} & z_{83} & z_{93} & z_{A3} & z_{B3} & z_{C3} & z_{D3} & z_{E3} & z_{F3} & z_{G3} \\
z_{14} & z_{24} & z_{34} & z_{44} & z_{54} & z_{64} & z_{74} & z_{84} & z_{94} & z_{A4} & z_{B4} & z_{C4} & z_{D4} & z_{E4} & z_{F4} & z_{G4} \\
z_{15} & z_{25} & z_{35} & z_{45} & z_{55} & z_{65} & z_{75} & z_{85} & z_{95} & z_{A5} & z_{B5} & z_{C5} & z_{D5} & z_{E5} & z_{F5} & z_{G5} \\
z_{16} & z_{26} & z_{36} & z_{46} & z_{56} & z_{66} & z_{76} & z_{86} & z_{96} & z_{A6} & z_{B6} & z_{C6} & z_{D6} & z_{E6} & z_{F6} & z_{G6} \\
z_{17} & z_{27} & z_{37} & z_{47} & z_{57} & z_{67} & z_{77} & z_{87} & z_{97} & z_{A7} & z_{B7} & z_{C7} & z_{D7} & z_{E7} & z_{F7} & z_{G7} \\
z_{18} & z_{28} & z_{38} & z_{48} & z_{58} & z_{68} & z_{78} & z_{88} & z_{98} & z_{A8} & z_{B8} & z_{C8} & z_{D8} & z_{E8} & z_{F8} & z_{G8} \\
z_{19} & z_{29} & z_{39} & z_{49} & z_{95} & z_{69} & z_{79} & z_{89} & z_{99} & z_{A9} & z_{B9} & z_{C9} & z_{D9} & z_{E9} & z_{F9} & z_{G9} \\
z_{1A} & z_{2A} & z_{3A} & z_{4A} & z_{5A} & z_{6A} & z_{7A} & z_{8A} & z_{9A} & z_{AA} & z_{BA} & z_{CA} & z_{DA} & z_{EA} & z_{FA} & z_{GA} \\
z_{1B} & z_{2B} & z_{3B} & z_{4B} & z_{5B} & z_{6B} & z_{7B} & z_{8B} & z_{9B} & z_{AB} & z_{BB} & z_{CB} & z_{DB} & z_{EB} & z_{FB} & z_{GB} \\
z_{1C} & z_{2C} & z_{3C} & z_{4C} & z_{5C} & z_{6C} & z_{7C} & z_{8C} & z_{9C} & z_{AC} & z_{BC} & z_{CC} & z_{DC} & z_{EC} & z_{FC} & z_{GC} \\
z_{1D} & z_{2D} & z_{3D} & z_{4D} & z_{5D} & z_{6D} & z_{7D} & z_{8D} & z_{9D} & z_{AD} & z_{BD} & z_{CD} & z_{DD} & z_{ED} & z_{FD} & z_{GD} \\
z_{1E} & z_{2E} & z_{3E} & z_{4E} & z_{5E} & z_{6E} & z_{7E} & z_{8E} & z_{9E} & z_{AE} & z_{BE} & z_{CE} & z_{DE} & z_{EE} & z_{FE} & z_{GE} \\
z_{1F} & z_{2F} & z_{3F} & z_{4F} & z_{5F} & z_{6F} & z_{7F} & z_{8F} & z_{9F} & z_{AF} & z_{BF} & z_{CF} & z_{DF} & z_{EF} & z_{FF} & z_{FG} \\
z_{1G} & z_{2G} & z_{3G} & z_{4G} & z_{5G} & z_{6G} & z_{7G} & z_{8G} & z_{9G} & z_{AG} & z_{BG} & z_{CG} & z_{DG} & z_{EG} & z_{FG} & z_{GG}
\end{pmatrix}_{16\times16}$$

Shift Column: In this part, it performs a cyclic shift in some columns of the matrix:

- the first column is unchanged.
- the second column is cyclically shifted one byte to the up
- the third column is cyclically shifted two bytes
- the fourth column is cyclically shifted three bytes…

This transformation is shown in Table 10.

Table 10. Shift Column matrix

$$\begin{pmatrix}
z_{11} & z_{2G} & z_{3F} & z_{4E} & z_{5D} & z_{6C} & z_{7B} & z_{8A} & z_{99} & z_{A8} & z_{B7} & z_{C6} & z_{D5} & z_{E4} & z_{F3} & z_{G2} \\
z_{12} & z_{21} & z_{3G} & z_{4F} & z_{5E} & z_{6D} & z_{7C} & z_{8B} & z_{9A} & z_{A9} & z_{B8} & z_{C7} & z_{D6} & z_{E5} & z_{F4} & z_{G3} \\
z_{13} & z_{22} & z_{31} & z_{4G} & z_{5F} & z_{6E} & z_{7D} & z_{8C} & z_{9B} & z_{AA} & z_{B9} & z_{C8} & z_{D7} & z_{E6} & z_{F5} & z_{G4} \\
z_{14} & z_{23} & z_{32} & z_{41} & z_{5G} & z_{6F} & z_{7E} & z_{8D} & z_{9C} & z_{AB} & z_{BA} & z_{C9} & z_{D8} & z_{E7} & z_{F6} & z_{G5} \\
z_{15} & z_{24} & z_{33} & z_{42} & z_{51} & z_{6G} & z_{7F} & z_{8E} & z_{9D} & z_{AC} & z_{BB} & z_{CA} & z_{D9} & z_{E8} & z_{F7} & z_{G6} \\
z_{16} & z_{25} & z_{34} & z_{43} & z_{52} & z_{61} & z_{7G} & z_{8F} & z_{9E} & z_{AD} & z_{BC} & z_{CB} & z_{DA} & z_{E9} & z_{F8} & z_{G7} \\
z_{17} & z_{26} & z_{35} & z_{44} & z_{53} & z_{62} & z_{71} & z_{8G} & z_{9F} & z_{AE} & z_{BD} & z_{CC} & z_{DB} & z_{EA} & z_{F9} & z_{G8} \\
z_{18} & z_{27} & z_{36} & z_{45} & z_{54} & z_{63} & z_{72} & z_{81} & z_{9G} & z_{AF} & z_{BE} & z_{CD} & z_{DC} & z_{EB} & z_{FA} & z_{G9} \\
z_{19} & z_{28} & z_{37} & z_{46} & z_{55} & z_{64} & z_{73} & z_{82} & z_{91} & z_{AG} & z_{BF} & z_{CE} & z_{DD} & z_{EC} & z_{FB} & z_{GA} \\
z_{1A} & z_{29} & z_{38} & z_{47} & z_{56} & z_{65} & z_{74} & z_{83} & z_{92} & z_{A1} & z_{BG} & z_{CF} & z_{DE} & z_{ED} & z_{FC} & z_{GB} \\
z_{1B} & z_{2A} & z_{39} & z_{48} & z_{57} & z_{66} & z_{75} & z_{84} & z_{93} & z_{A2} & z_{B1} & z_{CG} & z_{DF} & z_{EE} & z_{FD} & z_{GC} \\
z_{1C} & z_{2B} & z_{3A} & z_{49} & z_{58} & z_{67} & z_{76} & z_{85} & z_{94} & z_{A3} & z_{B2} & z_{C1} & z_{DG} & z_{EF} & z_{FE} & z_{GD} \\
z_{1D} & z_{2C} & z_{3B} & z_{4A} & z_{95} & z_{68} & z_{77} & z_{86} & z_{95} & z_{A4} & z_{B3} & z_{C2} & z_{D1} & z_{EG} & z_{FF} & z_{GE} \\
z_{1E} & z_{2D} & z_{3C} & z_{4B} & z_{5A} & z_{69} & z_{78} & z_{87} & z_{96} & z_{A5} & z_{B4} & z_{C3} & z_{D2} & z_{E1} & z_{FG} & z_{GF} \\
z_{1F} & z_{2E} & z_{3D} & z_{4C} & z_{5B} & z_{6A} & z_{79} & z_{88} & z_{97} & z_{A6} & z_{B5} & z_{C4} & z_{D3} & z_{E2} & z_{F1} & z_{GG} \\
z_{1G} & z_{2F} & z_{3E} & z_{4D} & z_{5C} & z_{6B} & z_{7A} & z_{89} & z_{98} & z_{A7} & z_{B6} & z_{C5} & z_{D4} & z_{E3} & z_{F2} & z_{G1}
\end{pmatrix}_{16\times16}$$

Inverse Reaction: This step performs the inverse reaction of 16×16 matrix. This transformation is shown in Table 11.

Table 11. Inverse Reaction matrix

$$\begin{pmatrix}
z_{G1} & z_{GG} & z_{GF} & z_{GE} & z_{GD} & z_{GC} & z_{GB} & z_{GA} & z_{G9} & z_{G8} & z_{G7} & z_{G6} & z_{G5} & z_{G4} & z_{G3} & z_{G2} \\
z_{F2} & z_{F1} & z_{FG} & z_{FF} & z_{FE} & z_{FD} & z_{FC} & z_{FB} & z_{FA} & z_{F9} & z_{F8} & z_{F7} & z_{F6} & z_{F5} & z_{F4} & z_{F3} \\
z_{E3} & z_{E2} & z_{E1} & z_{EG} & z_{EF} & z_{EE} & z_{ED} & z_{EC} & z_{EB} & z_{EA} & z_{E9} & z_{E8} & z_{E7} & z_{E6} & z_{E5} & z_{E4} \\
z_{D4} & z_{D3} & z_{D2} & z_{D1} & z_{DG} & z_{DF} & z_{DE} & z_{DD} & z_{DC} & z_{DB} & z_{DA} & z_{D9} & z_{D8} & z_{D7} & z_{D6} & z_{D5} \\
z_{C5} & z_{C4} & z_{C3} & z_{C2} & z_{C1} & z_{CG} & z_{CF} & z_{CE} & z_{CD} & z_{CC} & z_{CB} & z_{CA} & z_{C9} & z_{C8} & z_{C7} & z_{C6} \\
z_{B6} & z_{B5} & z_{B4} & z_{B3} & z_{B2} & z_{B1} & z_{BG} & z_{BF} & z_{BE} & z_{BD} & z_{BC} & z_{BB} & z_{BA} & z_{B9} & z_{B8} & z_{B7} \\
z_{A7} & z_{A6} & z_{A5} & z_{A4} & z_{A3} & z_{A2} & z_{A1} & z_{AG} & z_{AF} & z_{AE} & z_{AD} & z_{AC} & z_{AB} & z_{AA} & z_{A9} & z_{A8} \\
z_{98} & z_{97} & z_{96} & z_{95} & z_{94} & z_{93} & z_{92} & z_{91} & z_{9G} & z_{9F} & z_{9E} & z_{9D} & z_{9C} & z_{9B} & z_{9A} & z_{99} \\
z_{89} & z_{88} & z_{87} & z_{86} & z_{85} & z_{84} & z_{83} & z_{82} & z_{81} & z_{8G} & z_{8F} & z_{8E} & z_{8D} & z_{8C} & z_{8B} & z_{8A} \\
z_{7A} & z_{79} & z_{78} & z_{77} & z_{76} & z_{75} & z_{74} & z_{73} & z_{72} & z_{71} & z_{7G} & z_{7F} & z_{7E} & z_{7D} & z_{7C} & z_{7B} \\
z_{6B} & z_{6A} & z_{69} & z_{68} & z_{67} & z_{66} & z_{65} & z_{64} & z_{63} & z_{62} & z_{61} & z_{6G} & z_{6F} & z_{6E} & z_{6D} & z_{6C} \\
z_{5C} & z_{5B} & z_{5A} & z_{59} & z_{58} & z_{57} & z_{56} & z_{55} & z_{54} & z_{53} & z_{52} & z_{51} & z_{5G} & z_{5F} & z_{5E} & z_{5D} \\
z_{4D} & z_{4C} & z_{4B} & z_{4A} & z_{45} & z_{48} & z_{47} & z_{46} & z_{45} & z_{44} & z_{43} & z_{42} & z_{41} & z_{4G} & z_{4F} & z_{4E} \\
z_{3E} & z_{3D} & z_{3C} & z_{3B} & z_{3A} & z_{39} & z_{38} & z_{37} & z_{36} & z_{35} & z_{34} & z_{33} & z_{32} & z_{31} & z_{3G} & z_{3F} \\
z_{2F} & z_{2E} & z_{2D} & z_{2C} & z_{2B} & z_{2A} & z_{29} & z_{28} & z_{27} & z_{26} & z_{25} & z_{24} & z_{23} & z_{22} & z_{21} & z_{2G} \\
z_{1G} & z_{1F} & z_{1E} & z_{1D} & z_{1C} & z_{1B} & z_{1A} & z_{19} & z_{18} & z_{17} & z_{16} & z_{15} & z_{14} & z_{13} & z_{12} & z_{11}
\end{pmatrix}_{16\times16}$$

Add Round Key: Round key 1 obtained by the key algorithm and the last matrix obtained by the inverse reaction are added with each other. The new matrix that is formed goes into the loop again, and goes to 4. AddRoundkey and processes it with Roundkey2. So the cycle takes

place 15 times the same process. In the last step, it is processed with roundkey16 and encrypted.

Key Algorithm

In this section, we show how to create a key. First, let's consider a rcon matrix as in Table 12.

Table 12. Rcon matrix

$$\begin{pmatrix}
k_{11} & k_{12} & k_{13} & k_{14} & k_{15} & k_{16} & k_{17} & k_{18} & k_{19} & k_{1A} & k_{1B} & k_{1C} & k_{1D} & k_{1E} & k_{1F} & k_{1G} \\
k_{21} & k_{22} & k_{23} & k_{24} & k_{25} & k_{26} & k_{27} & k_{28} & k_{29} & k_{2A} & k_{2B} & k_{2C} & k_{2D} & k_{2E} & k_{2F} & k_{2G} \\
k_{31} & k_{32} & k_{33} & k_{34} & k_{35} & k_{36} & k_{37} & k_{38} & k_{39} & k_{3A} & k_{3B} & k_{3C} & k_{3D} & k_{3E} & k_{3F} & k_{3G} \\
k_{41} & k_{42} & k_{43} & k_{44} & k_{45} & k_{46} & k_{47} & k_{48} & k_{49} & k_{4A} & k_{4B} & k_{4C} & k_{4D} & k_{4E} & k_{4F} & k_{4G} \\
k_{51} & k_{52} & k_{53} & k_{54} & k_{55} & k_{56} & k_{57} & k_{58} & k_{59} & k_{5A} & k_{5B} & k_{5C} & k_{5D} & k_{5E} & k_{5F} & k_{5G} \\
k_{61} & k_{62} & k_{63} & k_{64} & k_{65} & k_{66} & k_{67} & k_{68} & k_{69} & k_{6A} & k_{6B} & k_{6C} & k_{6D} & k_{6E} & k_{6F} & k_{6G} \\
k_{71} & k_{72} & k_{73} & k_{74} & k_{75} & k_{76} & k_{77} & k_{78} & k_{79} & k_{7A} & k_{7B} & k_{7C} & k_{7D} & k_{7E} & k_{7F} & k_{7G} \\
k_{81} & k_{82} & k_{83} & k_{84} & k_{85} & k_{86} & k_{87} & k_{88} & k_{89} & k_{8A} & k_{8B} & k_{8C} & k_{8D} & k_{8E} & k_{8F} & k_{8G} \\
k_{91} & k_{92} & k_{93} & k_{94} & k_{95} & k_{96} & k_{97} & k_{98} & k_{99} & k_{9A} & k_{9B} & k_{9C} & k_{9D} & k_{9E} & k_{9F} & k_{9G} \\
k_{A1} & k_{A2} & k_{A3} & k_{A4} & k_{A5} & k_{A6} & k_{A7} & k_{A8} & k_{A9} & k_{AA} & k_{AB} & k_{AC} & k_{AD} & k_{AE} & k_{AF} & k_{AG} \\
k_{B1} & k_{B2} & k_{B3} & k_{B4} & k_{B5} & k_{B6} & k_{B7} & k_{B8} & k_{B9} & k_{BA} & k_{BB} & k_{BC} & k_{BD} & k_{BE} & k_{BF} & k_{BG} \\
k_{C1} & k_{C2} & k_{C3} & k_{C4} & k_{C5} & k_{C6} & k_{C7} & k_{C8} & k_{C9} & k_{CA} & k_{CB} & k_{CC} & k_{CD} & k_{CE} & k_{CF} & k_{CG} \\
k_{D1} & k_{D2} & k_{D3} & k_{D4} & k_{D5} & k_{D6} & k_{D7} & k_{D8} & k_{D9} & k_{DA} & k_{DB} & k_{DC} & k_{DD} & k_{DE} & k_{DF} & k_{DG} \\
k_{E1} & k_{E2} & k_{E3} & k_{E4} & k_{E5} & k_{E6} & k_{E7} & k_{E8} & k_{E9} & k_{EA} & k_{EB} & k_{EC} & k_{ED} & k_{EE} & k_{EF} & k_{EG} \\
k_{F1} & k_{F2} & k_{F3} & k_{F4} & k_{F5} & k_{F6} & k_{F7} & k_{F8} & k_{F9} & k_{FA} & k_{FB} & k_{FC} & k_{FD} & k_{FE} & k_{FF} & k_{FG} \\
k_{G1} & k_{G2} & k_{G3} & k_{G4} & k_{G5} & k_{G6} & k_{G7} & k_{G8} & k_{G9} & k_{GA} & k_{GB} & k_{GC} & k_{GD} & k_{GE} & k_{GF} & k_{GG}
\end{pmatrix}$$

1.Step. The following shifts are performed in the first and sixteenth columns of the input 16×16 matrix.

- the first column is cyclically shifted one value to the up
- sixteenth column is cyclically shifted one value to the down

This transformation is shown in Table 13.

Table 13. Shifted cipher key matrix

$$\begin{pmatrix} y_{G1} & y_{12} & y_{13} & y_{14} & y_{15} & y_{16} & y_{17} & y_{18} & y_{19} & y_{1A} & y_{1B} & y_{1C} & y_{1D} & y_{1E} & y_{1F} & y_{2G} \\ y_{11} & y_{22} & y_{23} & y_{24} & y_{25} & y_{26} & y_{27} & y_{28} & y_{29} & y_{2A} & y_{2B} & y_{2C} & y_{2D} & y_{2E} & y_{2F} & y_{3G} \\ y_{21} & y_{32} & y_{33} & y_{34} & y_{35} & y_{36} & y_{37} & y_{38} & y_{39} & y_{3A} & y_{3B} & y_{3C} & y_{3D} & y_{3E} & y_{3F} & y_{4G} \\ y_{31} & y_{42} & y_{43} & y_{44} & y_{45} & y_{46} & y_{47} & y_{48} & y_{49} & y_{4A} & y_{4B} & y_{4C} & y_{4D} & y_{4E} & y_{4F} & y_{5G} \\ y_{41} & y_{52} & y_{53} & y_{54} & y_{55} & y_{56} & y_{57} & y_{58} & y_{59} & y_{5A} & y_{5B} & y_{5C} & y_{5D} & y_{5E} & y_{5F} & y_{6G} \\ y_{51} & y_{62} & y_{63} & y_{64} & y_{65} & y_{66} & y_{67} & y_{68} & y_{69} & y_{6A} & y_{6B} & y_{6C} & y_{6D} & y_{6E} & y_{6F} & y_{7G} \\ y_{61} & y_{72} & y_{73} & y_{74} & y_{75} & y_{76} & y_{77} & y_{78} & y_{79} & y_{7A} & y_{7B} & y_{7C} & y_{7D} & y_{7E} & y_{7F} & y_{8G} \\ y_{71} & y_{82} & y_{83} & y_{84} & y_{85} & y_{86} & y_{87} & y_{88} & y_{89} & y_{8A} & y_{8B} & y_{8C} & y_{8D} & y_{8E} & y_{8F} & y_{9G} \\ y_{81} & y_{92} & y_{93} & y_{94} & y_{95} & y_{96} & y_{97} & y_{98} & y_{99} & y_{9A} & y_{9B} & y_{9C} & y_{9D} & y_{9E} & y_{9F} & y_{AG} \\ y_{91} & y_{A2} & y_{A3} & y_{A4} & y_{A5} & y_{A6} & y_{A7} & y_{A8} & y_{A9} & y_{AA} & y_{AB} & y_{AC} & y_{AD} & y_{AE} & y_{AF} & y_{BG} \\ y_{A1} & y_{B2} & y_{B3} & y_{B4} & y_{B5} & y_{B6} & y_{B7} & y_{B8} & y_{B9} & y_{BA} & y_{BB} & y_{BC} & y_{BD} & y_{BE} & y_{BF} & y_{CG} \\ y_{B1} & y_{C2} & y_{C3} & y_{C4} & y_{C5} & y_{C6} & y_{C7} & y_{C8} & y_{C9} & y_{CA} & y_{CB} & y_{CC} & y_{CD} & y_{CE} & y_{CF} & y_{DG} \\ y_{C1} & y_{D2} & y_{D3} & y_{D4} & y_{D5} & y_{D6} & y_{D7} & y_{D8} & y_{D9} & y_{DA} & y_{DB} & y_{DC} & y_{DD} & y_{DE} & y_{DF} & y_{EG} \\ y_{D1} & y_{E2} & y_{E3} & y_{E4} & y_{E5} & y_{E6} & y_{E7} & y_{E8} & y_{E9} & y_{EA} & y_{EB} & y_{EC} & y_{ED} & y_{EE} & y_{EF} & y_{FG} \\ y_{E1} & y_{F2} & y_{F3} & y_{F4} & y_{F5} & y_{F6} & y_{F7} & y_{F8} & y_{F9} & y_{FA} & y_{FB} & y_{FC} & y_{FD} & y_{FE} & y_{FF} & y_{GG} \\ y_{F1} & y_{G2} & y_{G3} & y_{G4} & y_{G5} & y_{G6} & y_{G7} & y_{G8} & y_{G9} & y_{GA} & y_{GB} & y_{GC} & y_{GD} & y_{GE} & y_{GF} & y_{1G} \end{pmatrix}_{16\times16}$$

Then, the first and the sixteenth columns of the matrix in Table 13 are added with the first column of the rcon matrix. So, we reach in Table 14.

Table 14. Adding column matrices

$$\begin{pmatrix} y_{G1} \\ y_{11} \\ y_{21} \\ y_{31} \\ y_{41} \\ y_{51} \\ y_{61} \\ y_{71} \\ y_{81} \\ y_{91} \\ y_{A1} \\ y_{B1} \\ y_{C1} \\ y_{D1} \\ y_{E1} \\ y_{F1} \end{pmatrix} + \begin{pmatrix} y_{2G} \\ y_{3G} \\ y_{4G} \\ y_{5G} \\ y_{6G} \\ y_{7G} \\ y_{8G} \\ y_{9G} \\ y_{AG} \\ y_{BG} \\ y_{CG} \\ y_{DG} \\ y_{EG} \\ y_{FG} \\ y_{GG} \\ y_{1G} \end{pmatrix} + \begin{pmatrix} k_{11} \\ k_{21} \\ k_{31} \\ k_{41} \\ k_{51} \\ k_{61} \\ k_{71} \\ k_{81} \\ k_{91} \\ k_{A1} \\ k_{B1} \\ k_{C1} \\ k_{D1} \\ k_{E1} \\ k_{F1} \\ k_{G1} \end{pmatrix} = \begin{pmatrix} y_{1H} \\ y_{2H} \\ y_{3H} \\ y_{4H} \\ y_{5H} \\ y_{6H} \\ y_{7H} \\ y_{8H} \\ y_{9H} \\ y_{AH} \\ y_{BH} \\ y_{CH} \\ y_{DH} \\ y_{EH} \\ y_{FH} \\ y_{GH} \end{pmatrix}, \begin{pmatrix} y_{12} \\ y_{22} \\ y_{32} \\ y_{42} \\ y_{52} \\ y_{62} \\ y_{72} \\ y_{82} \\ y_{92} \\ y_{A2} \\ y_{B2} \\ y_{C2} \\ y_{D2} \\ y_{E2} \\ y_{F2} \\ y_{G2} \end{pmatrix} + \begin{pmatrix} y_{1H} \\ y_{2H} \\ y_{3H} \\ y_{4H} \\ y_{5H} \\ y_{6H} \\ y_{7H} \\ y_{8H} \\ y_{9H} \\ y_{AH} \\ y_{BH} \\ y_{CH} \\ y_{DH} \\ y_{EH} \\ y_{FH} \\ y_{GH} \end{pmatrix} = \begin{pmatrix} y_{1I} \\ y_{2I} \\ y_{3I} \\ y_{4I} \\ y_{5I} \\ y_{6I} \\ y_{7I} \\ y_{8I} \\ y_{9I} \\ y_{AI} \\ y_{BI} \\ y_{CI} \\ y_{DI} \\ y_{EI} \\ y_{FI} \\ y_{GI} \end{pmatrix}, \begin{pmatrix} y_{13} \\ y_{23} \\ y_{33} \\ y_{43} \\ y_{53} \\ y_{63} \\ y_{73} \\ y_{83} \\ y_{93} \\ y_{A3} \\ y_{B3} \\ y_{C3} \\ y_{D3} \\ y_{E3} \\ y_{F3} \\ y_{G3} \end{pmatrix} + \begin{pmatrix} y_{1I} \\ y_{2I} \\ y_{3I} \\ y_{4I} \\ y_{5I} \\ y_{6I} \\ y_{7I} \\ y_{8I} \\ y_{9I} \\ y_{AI} \\ y_{BI} \\ y_{CI} \\ y_{DI} \\ y_{EI} \\ y_{FI} \\ y_{GI} \end{pmatrix} = \begin{pmatrix} y_{1J} \\ y_{2J} \\ y_{3J} \\ y_{4J} \\ y_{5J} \\ y_{6J} \\ y_{7J} \\ y_{8J} \\ y_{9J} \\ y_{AJ} \\ y_{BJ} \\ y_{CJ} \\ y_{DJ} \\ y_{EJ} \\ y_{FJ} \\ y_{GJ} \end{pmatrix}, \ldots$$

By the continuation of the process above, the round key 1 is generated as in Table 15.

Table 15. Round key 1 matrix

$$\begin{pmatrix} y_{1H} & y_{1I} & y_{1J} & y_{1K} & y_{1L} & y_{1M} & y_{1N} & y_{1O} & y_{1P} & y_{1Q} & y_{1R} & y_{1S} & y_{1T} & y_{1U} & y_{1V} & y_{1W} \\ y_{21H} & y_{2I} & y_{2J} & y_{2K} & y_{2L} & y_{2M} & y_{2N} & y_{2O} & y_{2P} & y_{2Q} & y_{2R} & y_{2S} & y_{2T} & y_{2U} & y_{2V} & y_{2W} \\ y_{3H} & y_{3I} & y_{3J} & y_{3K} & y_{3L} & y_{3M} & y_{3N} & y_{3O} & y_{3P} & y_{3Q} & y_{3R} & y_{3S} & y_{3T} & y_{3U} & y_{3V} & y_{3W} \\ y_{4H} & y_{4I} & y_{4J} & y_{4K} & y_{4L} & y_{4M} & y_{4N} & y_{4O} & y_{4P} & y_{4Q} & y_{4R} & y_{4S} & y_{4T} & y_{4U} & y_{4V} & y_{4W} \\ y_{5H} & y_{5I} & y_{5J} & y_{5K} & y_{5L} & y_{5M} & y_{5N} & y_{5O} & y_{5P} & y_{5Q} & y_{5R} & y_{5S} & y_{5T} & y_{5U} & y_{5V} & y_{5W} \\ y_{6H} & y_{6I} & y_{6J} & y_{6K} & y_{6L} & y_{6M} & y_{6N} & y_{6O} & y_{6P} & y_{6Q} & y_{6R} & y_{6S} & y_{6T} & y_{6U} & y_{6V} & y_{6W} \\ y_{7H} & y_{7I} & y_{7J} & y_{7K} & y_{7L} & y_{7M} & y_{7N} & y_{7O} & y_{7P} & y_{7Q} & y_{7R} & y_{7S} & y_{7T} & y_{7U} & y_{7V} & y_{7W} \\ y_{8H} & y_{8I} & y_{8J} & y_{8K} & y_{8L} & y_{8M} & y_{8N} & y_{8O} & y_{8P} & y_{8Q} & y_{8R} & y_{8S} & y_{8T} & y_{8U} & y_{8V} & y_{8W} \\ y_{9H} & y_{9I} & y_{9J} & y_{9K} & y_{9L} & y_{9M} & y_{9N} & y_{9O} & y_{9P} & y_{9Q} & y_{9R} & y_{9S} & y_{9T} & y_{9U} & y_{9V} & y_{9W} \\ y_{AH} & y_{AI} & y_{A} & y_{AK} & y_{AL} & y_{AM} & y_{AN} & y_{AO} & y_{AP} & y_{AQ} & y_{AR} & y_{AS} & y_{AT} & y_{AU} & y_{AV} & y_{AW} \\ y_{BH} & y_{BI} & y_{BJ} & y_{BK} & y_{BL} & y_{BM} & y_{BN} & y_{BO} & y_{BP} & y_{BQ} & y_{BR} & y_{BS} & y_{BT} & y_{BU} & y_{BV} & y_{BW} \\ y_{CH} & y_{CI} & y_{CJ} & y_{CK} & y_{CL} & y_{CM} & y_{CN} & y_{CO} & y_{CP} & y_{CQ} & y_{CR} & y_{CS} & y_{CT} & y_{CU} & y_{CV} & y_{CW} \\ y_{DH} & y_{DI} & y_{DJ} & y_{DK} & y_{DL} & y_{DM} & y_{DN} & y_{DO} & y_{DP} & y_{DQ} & y_{DR} & y_{DS} & y_{DT} & y_{DU} & y_{DV} & y_{DW} \\ y_{EH} & y_{EI} & y_{EJ} & y_{EK} & y_{EL} & y_{EM} & y_{EN} & y_{EO} & y_{EP} & y_{EQ} & y_{ER} & y_{ES} & y_{ET} & y_{EU} & y_{EV} & y_{EW} \\ y_{FH} & y_{FI} & y_{FJ} & y_{FK} & y_{FL} & y_{FM} & y_{FN} & y_{FO} & y_{FP} & y_{FQ} & y_{FR} & y_{FS} & y_{FT} & y_{FU} & y_{FV} & y_{FW} \\ y_{GH} & y_{GI} & y_{GJ} & y_{GK} & y_{GL} & y_{GM} & y_{GN} & y_{GO} & y_{GP} & y_{GQ} & y_{GR} & y_{GS} & y_{GT} & y_{GU} & y_{GV} & y_{GW} \end{pmatrix}$$

2.Step. In the newly formed round key 1, the first column is cyclically shifted one value to the up and sixteenth column is cyclically shifted one value to the down. Then, the elements of the first column, the sixteenth column of the type matrix and the second column of the Rcon matrix realize the addition with each other from the first row to sixteenth-row elements. By the continuation of the process in Table 16, the round key 2 is generated.

Table 16. Adding column matrices 2

$$\begin{pmatrix} y_{GH} \\ y_{1H} \\ y_{2H} \\ y_{3H} \\ y_{4H} \\ y_{5H} \\ y_{6H} \\ y_{7H} \\ y_{8H} \\ y_{9H} \\ y_{AH} \\ y_{BH} \\ y_{CH} \\ y_{DH} \\ y_{EH} \\ y_{FH} \end{pmatrix} + \begin{pmatrix} y_{2W} \\ y_{3W} \\ y_{4W} \\ y_{5W} \\ y_{6W} \\ y_{7W} \\ y_{8W} \\ y_{9W} \\ y_{AW} \\ y_{BW} \\ y_{CW} \\ y_{DW} \\ y_{EW} \\ y_{FW} \\ y_{GW} \\ y_{1W} \end{pmatrix} + \begin{pmatrix} k_{12} \\ k_{22} \\ k_{32} \\ k_{42} \\ k_{52} \\ k_{62} \\ k_{72} \\ k_{82} \\ k_{92} \\ k_{A2} \\ k_{B2} \\ k_{C2} \\ k_{D2} \\ k_{E2} \\ k_{F2} \\ k_{G2} \end{pmatrix} = \begin{pmatrix} y_{1X} \\ y_{2X} \\ y_{3X} \\ y_{4X} \\ y_{5X} \\ y_{6X} \\ y_{7X} \\ y_{8X} \\ y_{9X} \\ y_{AX} \\ y_{BX} \\ y_{CX} \\ y_{DX} \\ y_{EX} \\ y_{FX} \\ y_{GX} \end{pmatrix}, \begin{pmatrix} y_{1I} \\ y_{2I} \\ y_{3I} \\ y_{4I} \\ y_{5I} \\ y_{6I} \\ y_{7I} \\ y_{8I} \\ y_{9I} \\ y_{AI} \\ y_{BI} \\ y_{CI} \\ y_{DI} \\ y_{EI} \\ y_{FI} \\ y_{GI} \end{pmatrix} + \begin{pmatrix} y_{1X} \\ y_{2X} \\ y_{3X} \\ y_{4X} \\ y_{5X} \\ y_{6X} \\ y_{7X} \\ y_{8X} \\ y_{9X} \\ y_{AX} \\ y_{BX} \\ y_{CX} \\ y_{DX} \\ y_{EX} \\ y_{FX} \\ y_{GX} \end{pmatrix} = \begin{pmatrix} y_{1Y} \\ y_{2Y} \\ y_{3Y} \\ y_{4Y} \\ y_{5Y} \\ y_{6Y} \\ y_{7Y} \\ y_{8Y} \\ y_{9Y} \\ y_{AY} \\ y_{BY} \\ y_{CY} \\ y_{DY} \\ y_{EY} \\ y_{FY} \\ y_{GY} \end{pmatrix}, \begin{pmatrix} y_{1J} \\ y_{2J} \\ y_{3J} \\ y_{4J} \\ y_{5J} \\ y_{6J} \\ y_{7J} \\ y_{8J} \\ y_{9J} \\ y_{AJ} \\ y_{BJ} \\ y_{CJ} \\ y_{DJ} \\ y_{EJ} \\ y_{FJ} \\ y_{GJ} \end{pmatrix} + \begin{pmatrix} y_{1Y} \\ y_{2Y} \\ y_{3Y} \\ y_{4Y} \\ y_{5Y} \\ y_{6Y} \\ y_{7Y} \\ y_{8Y} \\ y_{9Y} \\ y_{AY} \\ y_{BY} \\ y_{CY} \\ y_{DY} \\ y_{EY} \\ y_{FY} \\ y_{GY} \end{pmatrix} = \begin{pmatrix} y_{1Z} \\ y_{2Z} \\ y_{3Z} \\ y_{4Z} \\ y_{5Z} \\ y_{6Z} \\ y_{7Z} \\ y_{8Z} \\ y_{9Z} \\ y_{AZ} \\ y_{BZ} \\ y_{CZ} \\ y_{DZ} \\ y_{EZ} \\ y_{FZ} \\ y_{GZ} \end{pmatrix}, \ldots$$

So, we reach other roundkeys by doing the other steps in this way.

The MES Encryption Process

MES decryption is similar to encryption in reverse order. In each cycle, the operations done in the encryption process are reversed,

- Add round key
- Inverse Reflection
- Shift collumns
- Transpose

Since sub-processes in each round are in reverse manner, the encryption and decryption algorithms needs to be separately implemented, although they are very closely related. So, The inverse of the 16×16 matrix key used in the MES encryption algorithm is taken in the computer environment and the encrypted text is decoded.

Conclusions

In this study, it investigates how an encryption algorithm obtains and how secure it would be by applying only matrix operations without using polynomials on the Galois finite field axioms and S-box table applied in the AES encryption algorithm. So, a new 256-bit encryption algorithm called matrix encryption standard (MES) obtain. Cipher key of its encryption algorithm decrypts in 2^{256} attempts.

References

[1] Avaroğlu, E., Dişkaya, O., and Menken, H. "The classıcal aes-lıke cryptology vıa the Fıbonaccı polynomıal matrıx". *Turkish journal of engineering*, *4*(3), 123-128, 2020.

[2] Ayres, F., and Jaisingh, L. R. "*Schaum's outline of theory and problems of abstract algebra"*. McGraw-Hill, 2004.

[3] Kak, Avi. "Lecture 8: AES: The advanced encryption standard." *Lecture Notes on'Computer and Network Security', Purdue University, URL: https://engineering. purdue. edu/kak/compsec/NewLectures/Lecture8. pdf* . 2016.

[4] Koc, C. K. "About cryptographic engineering." *Cryptographic engineering*. Springer, Boston, MA, 1-4, 2009.

[5] Paar, C., and Pelzl, J. "*Understanding cryptography: a textbook for students and practitioners"*. Springer Science & Business Media, 2009.

[6] Stinson, D. R., and Paterson, M. "*Cryptography: theory and practice"*. CRC press, 2018.