Malaysian Journal of Mathematical Sciences

Journal homepage: https://einspem.upm.edu.my/journal

An Efficient 2048-bit Block Cipher

Abu, N. A.*

Information Security Forensics and Computer Networking, Faculty of ICT, Universiti Teknikal Malaysia Melaka, Malaysia

E-mail: nura@utem.edu.my
**Corresponding author*

Received: 29 October 2020
Accepted: 5 July 2021

Abstract

An Advanced Encryption Standard (AES) has been the most popular block cipher in the last two decades. It has been extensively analyzed and efficiently implemented. Since 2000, an AES has been preset to be upgradable from the current 128-bit key to 192-bit key and finally 256-bit key on the same 128-bit plain text-cipher text block. A new call for 256-bit standard symmetric cipher is expected by 2030. Currently, an input file runs in kilobytes. It is apparent that a more practical cipher is much needed in handling daily task of protecting an important document from a user stand point of view without having to go through technical knowledge of encryption. A symmetric cipher has been traditionally operated on a small block. In this paper, however, a new proposal on a large 2048-bit block cipher using 256-bit key is presented.

Keywords: mega cipher, AES, symmetric cipher, block cipher.

1 Introduction

Following a classical concept of confusion and diffusion, an element of the cipher is represented by S-box and P-box respectively. In this paper, a new proposal of 256-bit key on a large 2048-bit block cipher is presented. From the 256-bit key, 3 round keys will be generated. A block cipher with a higher number of rounds in a block cipher is expected to produce better crunching effect. In this cipher, there will be only two rounds with an S and P-boxes in each round. At the same time, a mix column transformation will be invoked immediately right after each S or P-box. This megabit cipher requires at least two S-boxes and two P-boxes.

Previously, an encryption on a large plaintext input file will be done via a chain codebook. A large input will be divided into blocks of n-bits and encrypted sequentially one block at a time. In AES, 128-bit block[9] will be encrypted sequentially one block at a time. In this case, a cipher block size is 2048 bit. A key on a block should be kept running continuously. There should be no easy way to differentiate a running transmission whether it is just a key stream or it carries a ciphertext or not.

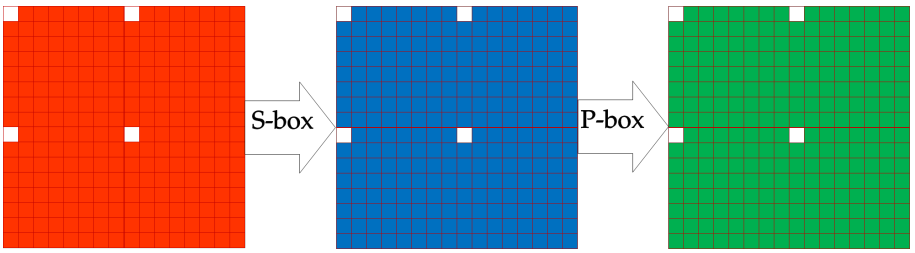

Figure 1: A 16×16 state array of bytes is compatible to any 16×16 S-box or P-box.

In this proposal, a large 2048-bit block shall be first presented as 16 by 16 state byte array. A state array represents the plaintext and is being processed to get the ciphertext. The state array will go through a process of byte substitution and permutation via S-box and P-box respectively as shown in Figure 1.

From a classical concept of substitution and transposition, an element of a cipher is represented by S-box and P-box respectively. Nevertheless, they are insufficient to produce an exhaustive avalanche effect. Thus, a distinct mix column transformation will be invoked immediately right after each S or P-box in each round.

While AES is employing an irreducible polynomial $m(x) = x^8 + x^4 + x^3 + x + 1$ with $m(2) = 283_{10}$, candidates of irreducible polynomials to be used in this instance are listed in Table 1. In this mega cipher, several irreducible polynomials will be employed.

Table 1: Candidates of irreducible polynomials to be used in this cipher.

i	$m_i(x)$	**Binary Coefficients**	**Decimal Value** $m_i(2)$
0	$x^8+x^4+x^3+x+1$	100011011_2	283_{10}
1	$x^8+x^5+x^3+x+1$	100101011_2	299_{10}
2	$x^8+x^6+x^4+x^3+x^2+x+1$	101011111_2	351_{10}
3	$x^8+x^6+x^5+x+1$	101100011_2	355_{10}
4	$x^8+x^6+x^5+x^2+1$	101100101_2	357_{10}
5	$x^8+x^6+x^5+x^3+1$	101101001_2	361_{10}
6	$x^8+x^7+x^6+x+1$	111000011_2	451_{10}
7	$x^8+x^7+x^6+x^5+x^2+x+1$	111100111_2	487_{10}

Traditionally, a session key will be used to pseudo-randomly generate round keys as a one-way process. A simple approach on a popular secure hashing algorithm may be called for here. Since the two round keys are coming from 24 consecutive hashing processes, the security of this cipher relies heavily on the strength of one-way function of SHA256.

1.1 Advanced Encryption Standard (AES)

Advanced Encryption Standard (AES) was specifically called for to replace the aging Data Encryption Standard (DES). Its selection procedure began back in (1997) by National Institute of Standards and Technology (NIST). When NIST summoned world's finest minds in the field of cryptography to cooperate by presenting their ideas for a new 128-bit encryption algorithm, RijnDael Algorithm was selected in the year 2000 [6].

Since the year 2000, an AES has been preset to be upgradable from the current 128-bit key to 192-bit key and finally 256-bit key on the same 128-bit plain text-cipher text block. However, an increase in the bit length of the key size while maintaining the block size will not increase full complexity the exhaustive brute force attack on the plaintext block. A new call for 256-bit standard symmetric cipher is expected by the year 2030.

AES consists of ten rounds of basic operations, namely, S-box, shift row, mixed column and exclusive-or with round keys. In order to achieve a full collusion, AES takes 4 rounds of operations. An efficient AES implementation will combine 4 rounds of operations into one large lookup table to be exclusive-ored with 4 round keys at once. The whole process of encryption or decryption will be cut down to 4 and a half rounds.

1.2 Optimization of AES cipher

A direct comparison with an equivalent version of AES by Dr. Brian Gladman original implementation in C language [7] has been made. Using 32-bit processor, it is possible to speed up execution of this cipher by combining the SubBytes and ShiftRows steps with the MixColumns step by transforming them into a sequence of table lookups. This combination requires four 256-entry 32-bit tables (together occupying 4096 bytes). A round can then be performed with 16 table lookup operations and twelve 32-bit exclusive-or operations, followed by four 32-bit exclusive-or operations in the AddRoundKey step [4]. Alternatively, the table lookup operation can be performed with a single 256-entry 32-bit table (occupying 1024 bytes) followed by circular rotation

operations.

By 2030 in the next call for standard cipher, a block and key is expected to be 256 bit. In this proposal, a large 2048-bit block is presented. Nevertheless, a 256-bit plaintext may also be feed into the large 2048-bit block. As such pseudo randomly generated Round Key 0 from a session key should be random enough to disguise many zeros within a plaintext file.

1.3 Substitution Bytes

An S-box maps a byte x into output byte, $y = S(x)$. Both the input and output are interpreted as polynomials over $GF(2)$. A substitution byte starts from converting an input byte into a polynomial over $GF(2^8)$. An inverse of this polynomial will become an input to go through an affine transformation. This mathematical arena is well known to have good non-linearity properties by applying an affine transformation to avoid attacks based on simple algebraic properties. The S-box is also used to avoid fixed points and opposite fixed points. An irreducible polynomial in AES is given by $m(x) = x^8 + x^4 + x^3 + x + 1$, or by $m(2) = 283_{10}$. Following similar technique, many more S-boxes can be generated from irreducible polynomials in Table 3.

Table 2: An affine transformation in AES S-box.

$$\begin{bmatrix} y_0 \\ y_1 \\ y_2 \\ y_3 \\ y_4 \\ y_5 \\ y_6 \\ y_7 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix}$$

1.4 Affine Transformation

An affine transformation is a polynomial multiplication modulo a predefined irreducible polynomial. An affine transform can be compactly presented here by $y = Ax \oplus b \pmod{m(x)}$, where A is a constant matrix of 8×8 bits, x represents the value to transform when b is a constant byte equal to $63_{16} = 01100011_2$ [6]. From an affine transform as shown in Table 2, it is possible to construct different S-boxes using different matrix A which is a non-singular matrix, b and irreducible polynomials $m(x)$.

An AES S-box in hexadecimal notation is given in Table 3 is the byte substitution modulo an irreducible polynomial $m_0(x)$ which carry the value $m_0(2) = 283_{10}$. Following similar technique, four more S-boxes have been generated from irreducible polynomials $m_1(x),\ m_2(x),\ m_6(x)$ and $m_7(x)$. There are tabulated as shown in Figures 4, 5, 6 and 7 respectively.

Table 3: An AES S-box in hexadecimal notation.

$x\backslash y$	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F
00	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
10	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
20	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
30	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
40	09	83	2C	1A	1B	6E	5A	A0	52	3b	D6	B3	29	E3	2F	84
50	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
60	d0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
70	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
80	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
90	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
A0	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
B0	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
C0	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
D0	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
E0	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
F0	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

1.5 Substitution Bytes (S-box) and Permutation Bytes (P-box)

Confusion is an important concept in symmetric block cipher. A cipher needs to completely obscure statistical properties of an original message. A bit change in a plaintext should cause on average fifty percent changes in the final ciphertext. An S-box and P-box transform blocks of byte input into byte output. S-box is a key-less fixed substitution cipher and contains permutation of 256 bytes and 8-bit values. Each input byte is mapped or replaced with a corresponding new byte in S-box. From 0 to 255 byte values, S-box is a one to one mapping to another byte. However, P-box is a permutation operation, without changing the output value, will change the index of the byte location.

Table 4: S-box 1 mod $m_1(x)$.

$x\backslash y$	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F
00	63	7C	7E	8A	7F	27	97	73	FF	8F	D3	36	8B	91	6B	A0
10	2D	DD	87	C1	3B	B2	5B	2E	17	55	1A	DB	67	50	10	E5
20	D6	02	AE	30	83	D7	32	8D	4F	16	19	71	ED	F4	57	EA
30	59	06	78	09	4D	E1	3F	D4	F3	58	68	93	48	25	20	2C
40	2B	45	41	D8	85	5E	CA	BD	13	49	AB	69	CB	33	86	1C
50	75	08	D9	BF	CC	BA	6A	4A	24	F1	A8	77	79	40	35	E2
60	EC	96	D1	5F	EE	AD	C4	54	74	C6	B0	3D	DF	A7	2A	F0
70	B9	07	6C	21	E6	A2	1B	F2	64	F6	D2	53	C2	92	56	5C
80	47	89	70	4C	E0	84	BE	2F	82	15	FD	EF	B7	8C	0C	43
90	C9	9F	E4	A3	95	5D	66	CE	37	0F	4B	05	03	1E	DC	C0
A0	FA	28	44	CF	3E	88	0D	FE	26	6D	1D	80	E7	8E	65	C5
B0	52	12	B8	C3	14	0A	FB	3C	6E	46	60	00	DA	B5	31	D0
C0	A4	5A	0B	9D	3A	F5	7D	B4	A5	29	04	EB	22	81	F8	94
D0	7A	AA	23	BC	18	B6	DE	AC	AF	9E	01	99	C7	9A	38	1F
E0	9C	E3	51	7B	76	62	42	61	A1	B1	11	0E	CD	6F	39	E8
F0	72	F7	A9	A6	BB	34	E9	4E	B3	98	9B	90	F9	D5	FC	C8

Table 5: P-box 1 mod $m_2(x)$.

$x\backslash y$	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F
00	63	7C	AA	ED	C1	E6	24	88	32	3A	A1	3F	86	33	96	64
10	CB	E5	CF	14	44	45	0B	AC	D7	3C	4B	54	DF	A8	A6	80
20	37	B9	20	A5	73	BC	D8	5E	F0	1D	70	A9	11	0A	84	2D
30	7F	A2	8A	65	31	4E	F8	99	7B	D9	C0	09	81	29	92	FA
40	0F	EB	48	69	C2	41	00	DE	6B	B8	8C	8E	BE	BA	FD	4D
50	EC	BF	5C	A7	EA	9E	40	CC	1C	CA	91	62	D6	C4	02	78
60	2B	35	C5	AE	97	21	26	82	4A	F3	F5	36	E8	FE	1E	52
70	6F	59	3E	3B	B2	03	10	BB	12	2E	46	B6	9B	25	E9	27
80	55	A0	61	30	B0	98	66	DA	B3	D0	34	58	94	AB	FB	72
90	67	EF	C8	75	D2	2F	D3	17	8D	D4	C9	CE	2C	E7	74	43
A0	A4	F4	0D	51	FC	A3	01	E2	E1	C3	DB	D1	B4	68	F2	5D
B0	DC	F7	B7	16	1A	39	E3	6C	FF	3D	F6	13	95	50	EE	5A
C0	47	2A	0E	1B	76	9A	85	57	5F	08	42	B5	87	90	93	7D
D0	B1	79	6D	56	28	9F	8F	AF	E0	19	AD	D5	DD	C7	BD	71
E0	23	6A	38	0C	8B	77	4F	7A	CD	7E	15	04	9C	18	49	E4
F0	9D	05	83	53	F1	5B	89	C6	1F	F9	06	22	60	6E	07	4C

Table 6: S-box 2 mod $m_6(x)$.

$x\backslash y$	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F
00	63	7C	D7	44	02	81	F0	F3	E8	13	12	24	91	74	10	C2
10	9D	2E	60	28	E0	F4	FB	6E	1A	DA	D3	61	E1	A1	B3	7F
20	27	45	FE	09	E2	C3	C6	0F	99	CE	A8	26	14	B0	DE	0A
30	E4	CF	BF	58	3B	A5	62	1C	19	B5	39	46	30	90	56	3C
40	7A	A9	70	35	AD	7B	6D	32	98	41	33	03	8A	52	55	C9
50	1E	D6	8E	F8	BD	A7	FA	88	D8	64	B1	6C	86	67	EC	21
60	A0	50	0E	53	0D	BA	C5	6A	4F	47	00	1D	E3	FD	DC	FC
70	65	BB	08	E5	4E	57	F1	FF	CA	48	9A	2A	F9	72	F7	84
80	EF	3E	3D	07	EA	2F	73	93	04	AF	6F	85	5F	76	CB	23
90	9E	1F	49	D4	4B	CC	68	69	97	17	C0	A3	78	D1	36	A2
A0	DD	D9	82	8D	AE	8C	95	3F	0C	9B	01	4A	94	8B	96	06
B0	BE	16	DB	BC	31	92	DF	C4	AA	89	5A	80	A4	B6	42	C8
C0	B9	F6	C1	25	D5	51	40	77	54	7E	B4	9C	0B	1B	E7	6B
D0	75	05	71	D0	E9	2B	5C	5E	18	D2	2C	7D	87	43	AC	37
E0	5B	5D	34	A6	ED	83	20	4D	F5	8F	79	4C	11	66	2D	E6
F0	B7	59	CD	22	9F	38	C7	B2	15	3A	EB	EE	29	B8	AB	F2

Table 7: P-box 2 mod $m_7(x)$.

x\y	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F
00	63	7C	18	31	2A	0A	4A	FA	C7	EB	23	AD	03	3A	5B	BB
10	C5	D4	D3	E8	43	50	04	54	A7	1D	CF	1B	8B	7E	FB	F9
20	C4	EA	4C	85	3B	86	52	97	87	FD	0E	B6	D0	4B	F8	1C
30	01	F2	5C	F1	C1	1A	AB	6B	17	D6	19	14	DB	9F	DA	8D
40	44	C6	53	A1	F4	9B	E4	37	4F	EE	65	57	0F	4E	ED	71
50	E5	21	2C	B4	D5	B5	89	C9	BA	3C	83	69	5A	CD	DC	EC
60	A6	26	5F	BC	FC	99	DE	12	32	68	2B	60	F3	EF	67	98
70	59	11	4D	DD	AA	29	D8	84	3F	10	E9	B1	BF	77	E0	82
80	F0	C3	45	CE	8F	90	F6	6F	A8	06	1F	15	A0	2D	BD	AF
90	75	B8	A5	B2	94	09	79	A3	55	3E	F5	80	24	E3	6A	02
A0	20	51	42	07	30	8E	88	C2	CC	B3	08	96	16	61	36	CA
B0	7B	6D	38	22	13	FF	66	40	0B	B7	C0	3D	48	62	A4	D9
C0	81	7F	35	00	7D	7A	8C	9C	AC	F7	1E	6E	49	A2	2F	6C
D0	CB	92	E6	28	47	39	E2	78	DF	27	25	E7	95	D7	9E	34
E0	8A	41	AE	70	74	33	C8	5E	73	91	46	A9	BE	9A	64	E1
F0	B9	58	2E	5D	D2	D1	FE	72	0D	05	9D	0C	56	B0	93	76

In this instance, $m_1(x)$ and $m_2(x)$ have been selected as the irreducible polynomials to generate S-box 1 and P-box 1 respectively. At the same time, $m_6(x)$ and $m_7(x)$ have been selected as the irreducible polynomials to generate S-box 2 and P-box 2 respectively. An S or P boxes will be generated from an input byte. A byte will be converted into a polynomial in $\mathbb{F}_2$. An inverse of the polynomial modulo irreducible polynomial $m_i(x)$ will go through an affine transform as prescribed in generation process of AES S-box.

1.6 MixColumn Operation

In original AES, a mixed column step is basically operated on four bytes of a state array [6]. Each element of the state matrix is multiplication matrix with the corresponding column of the polynomial matrix. Resulting in four bytes in one column will replaces the original column of the state array. A basic mix column is written in matrical equation as follows;

$$\begin{bmatrix} s'_0 \\ s'_1 \\ s'_2 \\ s'_3 \end{bmatrix} = \begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix} \begin{bmatrix} s_0 \\ s_1 \\ s_2 \\ s_3 \end{bmatrix}.$$

In a decryption process, an inverse of mix column operation can be viewed as follows;

$$\begin{bmatrix} s_0 \\ s_1 \\ s_2 \\ s_3 \end{bmatrix} = \begin{bmatrix} 14 & 11 & 13 & 19 \\ 19 & 14 & 11 & 13 \\ 13 & 19 & 14 & 11 \\ 11 & 13 & 19 & 14 \end{bmatrix} \begin{bmatrix} s'_0 \\ s'_1 \\ s'_2 \\ s'_3 \end{bmatrix}.$$

A product of two bytes will be computed as a product of two polynomials in finite field modulo an irreducible polynomial $m_i(x)$. Let us take a simple example:

$$\begin{aligned}
167_{10} \cdot 245_{10} \bmod 299_{10} &= \text{A7} \cdot \text{F5} \bmod \text{12B} \\
&= 10100111 \cdot 11110101 \bmod 100101011 \\
&= 112213253321211 \\
&= 110011011101011 \pmod 2 \\
&\oplus \quad \underline{100101011} \\
&= \quad 10110000101011 \\
&\oplus \quad \underline{100101011} \\
&= \quad 100101001011 \\
&\oplus \quad \underline{100101011} \\
&= \quad 10011 \pmod{100101011}.
\end{aligned}$$

From this simple example, it can be deduced that, this byte multiplication can be efficiently done in binary mode. An addition will take an exclusive-or of two bytes. Consequently, a mix column operation on a state array can be viewed as a product of two matrices between a mix column matrix and the state array.

$$\begin{bmatrix} s'_{0,0} & s'_{0,1} & s'_{0,2} & s'_{0,3} \\ s'_{1,0} & s'_{1,1} & s'_{1,2} & s'_{1,3} \\ s'_{2,0} & s'_{2,1} & s'_{2,2} & s'_{2,3} \\ s'_{3,0} & s'_{3,1} & s'_{3,2} & s'_{3,3} \end{bmatrix} = \begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix} \begin{bmatrix} s_{0,0} & s_{0,1} & s_{0,2} & s_{0,3} \\ s_{1,0} & s_{1,1} & s_{1,2} & s_{1,3} \\ s_{2,0} & s_{2,1} & s_{2,2} & s_{2,3} \\ s_{3,0} & s_{3,1} & s_{3,2} & s_{3,3} \end{bmatrix}.$$

It should be noted here that a product mix column matrix and its inverse will produce an identity matrix.

$$\begin{bmatrix} 14 & 11 & 13 & 19 \\ 19 & 14 & 11 & 13 \\ 13 & 19 & 14 & 11 \\ 11 & 13 & 19 & 14 \end{bmatrix} = \begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

A mix column is known to be the primary source of diffusion here. In this mega cipher, a larger setting is presented as a mix column operation as shown in Figure 2. A mix column matrix M has been chosen as a diagonal matrix.

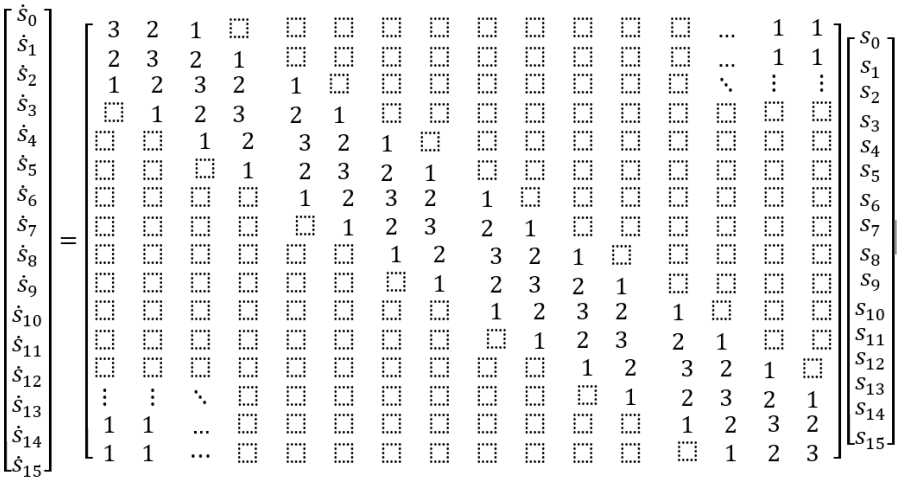

Figure 2: A mix column operation on 16×16 byte array.

In this cipher, each mix column operation will have different irreducible polynomials namely, $m_1(x), m_2(x), m_6(x) and m_7(x)$ respectively. Using the same mix column matrix M, there will be 4 different inverse mix column matrices as tabulated in Figure 8-11. An encryption process is typically set simpler in a more efficient mode than decryption. Here, a matrix multiplication on mix column matrix M has been preferably chosen during an encryption operation while an inversion will do the decryption. Both processes will require modular operation. In order to design an efficient cipher, a computationally friendly operation shall be preset in mind.

Table 8: An inverse mix column matrix M^{-1} mod $m_1(x)$.

2B	B0	76	69	5C	65	7E	55	7C	80	01	03	67	C4	62	05
B0	23	97	3A	A1	07	58	94	43	15	A6	CB	D7	4B	BF	62
76	97	5F	31	B2	C7	FB	A6	15	73	84	A1	89	9C	4B	C4
69	3A	31	89	B4	25	1F	A2	4E	A2	1F	25	B4	89	D7	67
5C	A1	B2	B4	A3	59	04	71	93	5A	36	B7	25	A1	CB	03
65	07	C7	25	59	0A	F2	0E	5E	C2	7A	36	1F	84	A6	01
7E	58	FB	1F	04	F2	4D	6E	EC	33	C2	5A	A2	73	15	80
55	94	A6	A2	71	0E	6E	51	FD	EC	5E	93	4E	15	43	7C
7C	43	15	4E	93	5E	EC	FD	51	6E	0E	71	A2	A6	94	55
80	15	73	A2	5A	C2	33	EC	6E	4D	F2	04	1F	FB	58	7E
01	A6	84	1F	36	7A	C2	5E	0E	F2	0A	59	25	C7	07	65
03	CB	A1	25	B7	36	5A	93	71	04	59	A3	B4	B2	A1	5C
67	D7	89	B4	25	1F	A2	4E	A2	1F	25	B4	89	31	3A	69
C4	4B	9C	89	A1	84	73	15	A6	FB	C7	B2	31	5F	97	76
62	BF	4B	D7	CB	A6	15	43	94	58	07	A1	3A	97	23	B0
05	62	C4	67	03	01	80	7C	55	7E	65	5C	69	76	B0	2B

Table 9: An inverse mix column matrix M^{-1} mod $m_2(x)$.

2A	03	18	23	DF	4C	52	D5	31	0E	C0	BE	24	B6	05	80
03	64	22	3E	A5	9E	E2	44	FC	8A	A3	2E	F1	23	60	05
18	22	16	0B	E3	4E	A5	BA	8E	7C	21	70	86	73	23	B6
23	3E	0B	30	28	C9	6F	4A	1F	5C	BE	41	09	86	F1	24
DF	A5	E3	28	29	E3	A4	14	46	5F	D6	F4	41	70	2E	BE
4C	9E	4E	C9	E3	9D	29	45	B9	7D	CC	D6	BE	21	A3	C0
52	E2	A5	6F	A4	29	14	B0	4A	42	7D	5F	5C	7C	8A	0E
D5	44	BA	4A	14	45	B0	47	17	4A	B9	46	1F	8E	FC	31
31	FC	8E	1F	46	B9	4A	17	47	B0	45	14	4A	BA	44	D5
0E	8A	7C	5C	5F	7D	42	4A	B0	14	29	A4	6F	A5	E2	52
C0	A3	21	BE	D6	CC	7D	B9	45	29	9D	E3	C9	4E	9E	4C
BE	2E	70	41	F4	D6	5F	46	14	A4	E3	29	28	E3	A5	DF
24	F1	86	09	41	BE	5C	1F	4A	6F	C9	28	30	0B	3E	23
B6	23	73	86	70	21	7C	8E	BA	A5	4E	E3	0B	16	22	18
05	60	23	F1	2E	A3	8A	FC	44	E2	9E	A5	3E	22	64	03
80	05	B6	24	BE	C0	0E	31	D5	52	4C	DF	23	18	03	2A

Table 10: An inverse mix column matrix M^{-1} mod $m_6(x)$.

50	4D	B5	B9	49	E5	DD	E0	4F	B8	0C	23	1C	19	20	0B
4D	FE	6E	83	A5	CD	1A	E8	22	5C	C2	E9	45	A6	09	20
B5	6E	49	16	E5	18	FC	B9	9A	5C	FB	46	37	D4	A6	19
B9	83	16	CA	C8	17	3E	6E	27	B8	1B	46	32	37	45	1C
49	A5	E5	C8	BE	C8	E5	A5	49	00	23	E9	46	46	E9	23
E5	CD	18	17	C8	EC	B5	41	01	34	52	23	1B	FB	C2	0C
DD	1A	FC	3E	E5	B5	0E	32	1F	15	34	00	B8	5C	5C	B8
E0	E8	B9	6E	A5	41	32	35	43	1F	01	49	27	9A	22	4F
4F	22	9A	27	49	01	1F	43	35	32	41	A5	6E	B9	E8	E0
B8	5C	5C	B8	00	34	15	1F	32	0E	B5	E5	3E	FC	1A	DD
0C	C2	FB	1B	23	52	34	01	41	B5	EC	C8	17	18	CD	E5
23	E9	46	46	E9	23	00	49	A5	E5	C8	BE	C8	E5	A5	49
1C	45	37	32	46	1B	B8	27	6E	3E	17	C8	CA	16	83	B9
19	A6	D4	37	46	FB	5C	9A	B9	FC	18	E5	16	49	6E	B5
20	09	A6	45	E9	C2	5C	22	E8	1A	CD	A5	83	6E	FE	4D
0B	20	19	1C	23	0C	B8	4F	E0	DD	E5	49	B9	B5	4D	50

Table 11: An inverse mix column matrix M^{-1} mod $m_7(x)$.

3A	35	A7	E9	0F	58	79	10	7F	5C	AC	2F	80	C9	B5	09
35	37	01	85	4B	E6	43	28	62	D8	E3	D6	CB	E8	6A	B5
A7	01	62	24	3C	6A	16	B5	0B	7C	98	57	39	1F	E8	C9
E9	85	24	2B	22	81	4A	C6	58	9D	85	50	73	39	CB	80
0F	4B	3C	22	41	BF	77	A4	53	87	E8	76	50	57	D6	2F
58	E6	6A	81	BF	DD	A0	36	AF	D7	1E	E8	85	98	E3	AC
79	43	16	4A	77	A0	07	15	0C	AD	D7	87	9D	7C	D8	5C
10	28	B5	C6	A4	36	15	18	32	0C	AF	53	58	0B	62	7F
7F	62	0B	58	53	AF	0C	32	18	15	36	A4	C6	B5	28	10
5C	D8	7C	9D	87	D7	AD	0C	15	07	A0	77	4A	16	43	79
AC	E3	98	85	E8	1E	D7	AF	36	A0	DD	BF	81	6A	E6	58
2F	D6	57	50	76	E8	87	53	A4	77	BF	41	22	3C	4B	0F
80	CB	39	73	50	85	9D	58	C6	4A	81	22	2B	24	85	E9
C9	E8	1F	39	57	98	7C	0B	B5	16	6A	3C	24	62	01	A7
B5	6A	E8	CB	D6	E3	D8	62	28	43	E6	4B	85	01	37	35
09	B5	C9	80	2F	AC	5C	7F	10	79	58	0F	E9	A7	35	3A

This large cipher has been designed for common input files ranging from 2048-bit which is 256 bytes onwards. Since a standard hash function will be used to generate the round keys, a variable length of session key is also feasible in this cipher. It is also practical to use password as a symmetric key. A minimum of 20-character password is recommended for this cipher. In order to achieve a minimum 120-bit strength 20 alphanumeric characters is currently sufficient to overcome a full brute-force attack.

In AES, all byte polynomial operations are done in a fixed finite field modulo an irreducible polynomial $m_0(x) = x^8 + x^4 + x^3 + x + 1$. In order to compensate a large plaintext block, 4 finite fields have been introduced into this mega cipher modulo 4 irreducible polynomials, specifically, $m_1(x), m_2(x), m_6(x)$and$m_7(x)$ as given in Table 1 Consequently, every element in S-box 1, P-Box 1, S-box 2 and P-box 2 has been generated from a ring modulo irreducible polynomials $m_1(x), m_2(x), m_6(x)$ and $m_7(x)$ respectively.

1.7 A Mega Block Cipher

A megabit block cipher is called for here in order to cater for practical needs. Currently, an input file runs in kilobytes. It is apparent a more practical cipher is much needed in handling daily task of protecting an important document from a user stand point of view without having to go through technical knowledge of encryption. As the current block cipher standard, AES has been well-studied cryptographic construction from which parts of AES are used in many cryptographic designs. A suitable design is sought here by simplifying the operation, increasing state array size and decreasing the number of rounds.

1.8 Round Key Generation

In this new proposal of a large symmetric cipher, Round Key 0, Round Key 1 and Round Key 2 may be pre-generated prior to an encryption or decryption process. Initially, a session key will go through hashing processes via SHA256 eight times to accumulate 2048-bit Round Key 0. First, the last 256-bit Round Key 0 will go through another SHA256 8 times in order to accumulate 2048-bit Round Key 1. Second, the last 256-bit Round Key 1 will go through SHA256 another 8 times in order to accumulate 2048-bit Round Key 2 as shown on the right hand side(RHS) of Figure 3. Each round key will be reshaped into 16 by 16 state byte array.

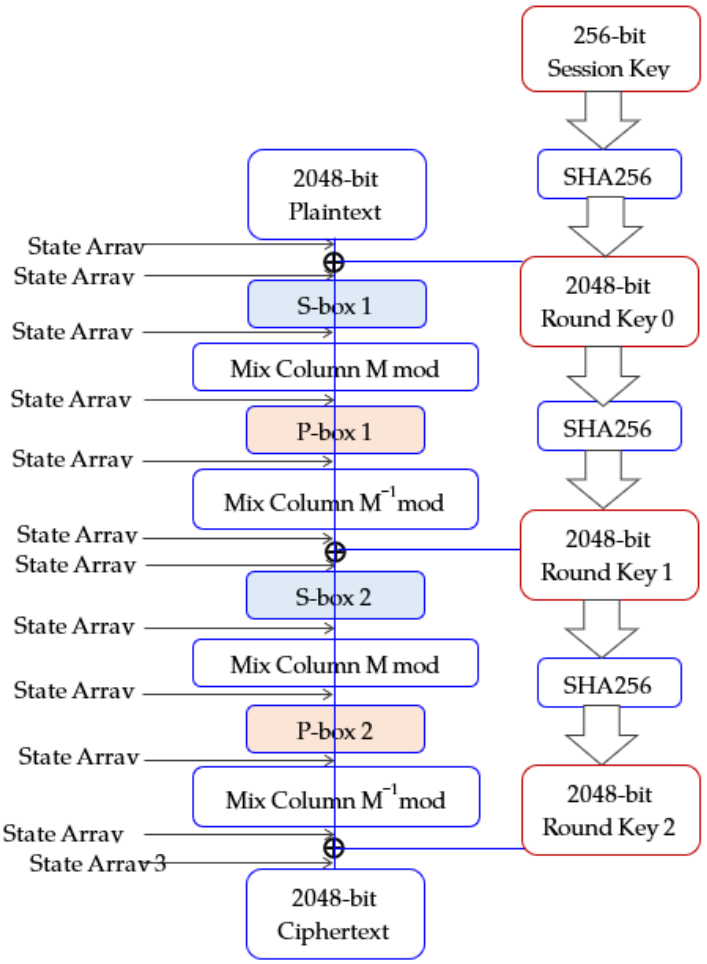

Figure 3: An overview structure of a megabit cipher.

1.9 Encryption Process

Initially, in Round 0, a 2048-bit plaintext will be reshaped into 16 by 16 state array of bytes. The state array will be exclusive-ored with Round Key 0. In Round 1, the state array will first go through S-box 1 and P-box 1. As depicted on the left hand side(LHS) of Figure 3, an incoming 16 by 16 state array will then be exclusive-ored with Round Key 1. Second, the state array will go through S-box 2 and P-box 2 in Round 2. The incoming 16 by 16 state array will then be exclusive-ored with Round Key 2.

Nevertheless, a mix column transformation will be injected into the encryption process immediately right after each S or P-box. A combination of S-box and P-box is not expected to provide sufficient full confusion and diffusion effects to this large mega cipher. There will be 4 mix column matrices here, namely, M mod $m_1(x)$, M^{-1} mod $m_2(x)$, M mod $m_6(x)$ and M^{-1} mod $m_7(x)$.

1.10 Decryption Process

Following an encryption process, Round Key 0, Round Key 1 and Round Key 2 may be pre-generated prior to a decryption process. There are also inverse boxes S^{-1}box1, S^{-1}box2, P^{-1}box1 and P^{-1}box2 being prescribed for a decryption process. In Round 0, a 2048-bit ciphertext will be reshaped into 16 by 16 state array of bytes. An incoming 16 by 16 state array will be initially exclusive-ored with Round Key 2. In Round 1, the state array will go through P^{-1}box2 and S^{-1}box2. The outgoing 16 by 16 state array will be exclusive-ored with Round Key 1. In round 2, the state array will go through P^{-1}box1 and S^{-1}box1 consecutively. Lastly, the state array will be exclusive-ored with Round Key 0 in order to produce an original 16 by 16 state array of plaintext bytes.

A mix column transformation will be invoked into the decryption process immediately right after each S or P-box. There are 4 mix column matrices here, namely, Mmod $m_7(x)$, M^{-1} mod $m_6(x)$, M mod $m_2(x)$ and M^{-1} mod $m_1(x)$.

1.11 Sample Input and Session Key

A simple plaintext has been chosen which takes byte values from 0 to 255. A state array will be shaped as 16 by 16 bytes column wise. A short session has also been chosen as 'abc' from original SHA256 proposal [10]. Every task description during the operational process on each state array has been prescribed in Figure 4. They have been pointed out on their locations in the overall design on this mega cipher in Figure 3.

Table 12: A task description on every state array.

State Array	Task Description	First Input Matrix	Second Input Matrix
0	Form initial column wise State Array	1D plaintext	
1.0	An exclusive-or against Round Key	State Array 0	Round Key 0
1.1	Byte Substitution operation	State Array 1.0	S-box 1
1.2	Mix Column Matrix Multiplication	M mod $m_1(x)$	State Array 1.1
1.3	Byte Permutation operation	State Array 1.2	P-box 1
1.4	Mix Column Matrix Multiplication	M^{-1} mod $m_2(x)$	State Array 1.3
2.0	An exclusive-or against Round Key	State Array 1.4	Round Key 1
2.1	Byte Substitution operation	State Array 2.0	S-box 2
2.2	Mix Column Matrix Multiplication	M^{-1} mod $m_3(x)$	State Array 2.1
2.3	Byte Permutation operation	State Array 2.2	P-box 2
2.4	Mix Column Matrix Multiplication	M mod $m_1(x)$	State Array 2.3
3.0	An exclusive-or against Round Key	State Array 2.4	Round Key 2

On one hand, step by step state array matrices during an encryption process of this Mega Cipher are given in Appendix 1. Next to the state array, another matrix on the next operation is also given. On another hand, step by step state array matrices during a decryption process of this Mega Cipher are given in Appendix 2.

At each stage, a 2048-bit plaintext will be presented as 16 by 16 state array of bytes. Every operation in this mega cipher has been also compactly represented as a 16 by 16 matrix of bytes. They are being tabulated in Appendices during an encryption and decryption processes.

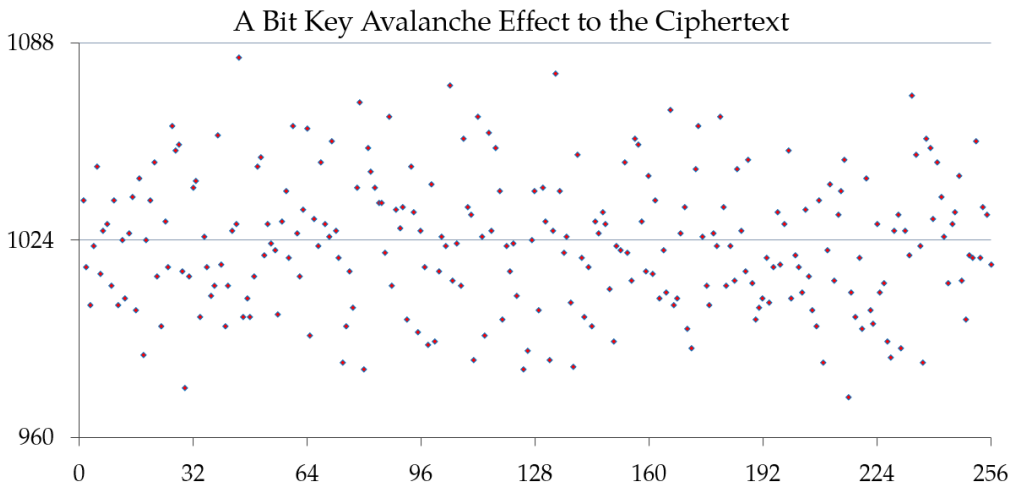

Figure 4: An avalanche effect of a bit change on the 256-bit session key.

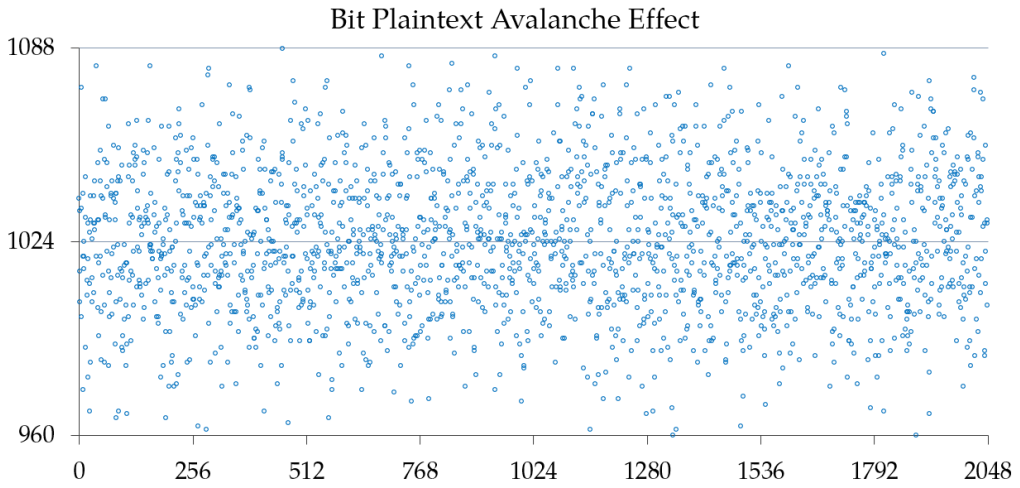

Figure 5: An avalanche effect from a bit change in the 2048-bit plaintext to the ciphertext.

1.12 An Avalanche Effect to the Ciphertext

A preliminary avalanche effect test on a bit change in the 256-bit session key has produced an average score of 1022.63 bits change on the ciphertext. The resulting bit changes in the ciphertext have been depicted in Figure 4. At the same time, an avalanche effect test on a bit change in the 2048-bit sample plaintext has produced an average score of 1024.55 bits change on the sample ciphertext. The resulting bit changes in the ciphertext have been depicted in Figure 5. This mega cipher has managed to achieve a strict avalanche criterion [5] in two rounds.

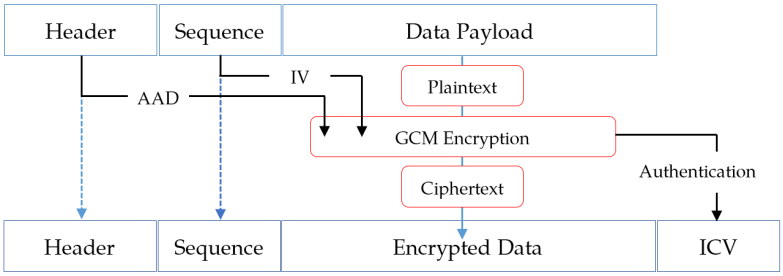

Figure 6: A network packet is encrypted and authenticated via a GCM.

1.13 Galois Counter Mode

Galois Counter Mode (GCM) is a block cipher mode [8]. It uses a universal hashing mechanism over a binary Galois field. Following an efficient speed of AES of 10 gigabits per second in hardware, GCM has filled a companion role in providing message authentication at such a high speed [1]. Another useful property is that it accepts an initialization vector (IV) of arbitrary length. In GCM, message authenticated encryption operation takes 4 inputs:

i. A secret key K.

ii. An initial vector V.

iii. A long plaintext P.

iv. An additional authenticated data A.

There will be 2 outputs:

i. A cipher text C.

ii. An authentication tag T.

Message authenticated encryption operation, however, takes 5 inputs:

i. A secret key K.

ii. An initial vector IV.

iii. A long ciphertext C.

iv. An additional authenticated data A.

v. An authentication tag T.

There will be only one single output: A plaintext value P or a special symbol FAIL that indicates that the inputs are not authentic. A primary purpose of an initial vector (IV) is to be a nonce, that is distinct for each invocation of any encryption operation for a fixed key. It is acceptable for an

IV to be randomly generated as long as the distinctness of the IV values is highly likely. An IV is authenticated and it is not necessary to include it in an additional authenticated data (AAD) field.

Given a plaintext, GCM provides both confidentiality and message authentication at the same time. The strength of the authentication of P, IV and A is determined by the length t of the authentication tag. When the length of P is zero, GCM acts as a MAC on an input A. The mode of operation that uses GCM as a stand-alone message authentication code is denoted as GMAC.

GCM uses an irreducible polynomial

$$f(x) = x^{128} + x^7 + x^2 + x + 1 = 100000000000000000000000000000087_{16}.$$

Therefore,

$$x^{128} \equiv x^7 + x^2 + x + 1 = 87_{16} \bmod f(x).$$

Using a typical cryptographic encapsulation, a network packet will be protected via a GCM encryption mode as shown in Figure 6. At the same time this mega is well suited for a GCM encryption mode in encrypting large files.

1.14 Elements of Niche Design

This cipher has been designed as a 2048-bit block cipher following current popular standard in public infrastructure RSA 2048 bits [3]. There are several languages around the globe which use more than 256 characters such as Chinese and Japanese. Current encoding in markup languages use more than two bytes to compose a text, images, or invisible control characters. A large block cipher is called for here.

A larger plaintext/ciphertext block will ease the use of counter encryption mode such as GCM in encrypting a large file. A variable length session key has been introduced as an initial input to a one-way secure hashing SHA256. This cipher is operating on a finite Galois field. It provides a compact mathematical support representing a cipher block in terms of state arrays. At the same time, a polynomial operation in this finite field provides an efficient computing arena.

1.15 Post Quantum Era

AES and NTRU have made use of polynomial prowess. Traditionally, it is more practical to operate and communicate on an integer ring. Operating on polynomials is more efficient and programming friendly. Practically, AES performs faster than NTRU cryptosystem. In the year 2000, a reference Rijndeal code in c++ can encrypt at 1 megabit per second. In the year 2010, an optimised c plus assembly language can encrypt at 1 gigabit per second. In the year 2020, a crypto chip of GCM-AES can perform an encryption at 10 Gigabit per second [1]. AES and NTRU are both expected to survive a full fledge quantum computer prowess.

Ajtai [2] proposed an idea of constructing a collision-free one-way function whose security on average is equivalent to hard approximation problems in lattices. During a round key generation in this mega cipher, a secure hashing algorithm from lattice cryptography is very much called for in post quantum era.

1.16 Future Attack

In this mega cipher, a larger 2048-bit plaintext/ciphertext has been introduced using a variable key length. There will be no technical restriction on the size of a password. A user will be encouraged to use at least 20 alphanumeric choice of password in order to reach current security level of 120 bits. From a practical design, this mega cipher has a potential to be popular cipher to non-technical users in various application. At the same time, it opens for new series of future attacks on its practical uses. A larger block size will certainly open a larger room for possible attack on this mega cipher. A strong and in-depth attack and cryptanalysis are very much welcomed here.

2 Conclusion

A secure cipher has always been designed and used by a technical user. It has been a serious challenge to deploy an encryption technique to a non-technical user in open masses. In this paper, a block cipher has been designed from its initial algorithm engine to encourage a typical user to use it as easy as a typical login. There will be a direct use of password to generate a session key. The block size of this mega cipher is also large enough to cater for daily use. This mega cipher is also designed to attain an optimal efficiency level for a block which will take only 2 rounds of confusion and diffusion operations. From a practical design, this mega cipher has a potential to be popular cipher to non-technical users in various application around the globe.

Acknowledgement We thank the reviewers for the constructive comments and editor for the guidance.

Conflicts of Interest The author declares no conflict of interest.

References

[1] N. Ahmad, M. W. Lim & M. H. Jabbar (2018). Advanced encryption standard with galois counter mode using field programmable gate array. In *Journal of Physics: Conference Series, 1st International Conference on Green and Sustainable Computing (ICoGeS)*, pp. 1–7. IOP Publishing Ltd, Kuching.

[2] M. Ajtai (1996). Generating hard instances of lattice problems. In *In Proceedings of the Twenty-Eighth Annual ACM Symposium on the Theory of Computing*, pp. 99–108. ACM, New York, NY.

[3] A. Barker & A. Roginsky (2019). *Transitioning the Use of Cryptographic Algorithms and Key Lengths*. NIST, United State, US.

[4] G. Bertoni, L. Breveglieri, P. Fragneto, M. Macchetti & S. Marchesin (2003). Efficient software implementation of aes on 32-bit platforms. In *Cryptographic Hardware and Embedded Systems - CHES 2002*, pp. 159–171. Springer, Berlin, Heidelberg.

[5] J. C. H. Castro, J. M. Sierra, A. Seznec, A. Izquierdo & A. Ribagorda (2005). The strict avalanche criterion randomness test. *Mathematics and Computers in Simulation*, *68*(1), 1–7.

[6] J. Daemen & V. Rijmen (2002). *The Design of Rijndael*. Springer, Berlin, Heidelberg.

[7] B. Galdman. *Cryptographic Technology Interests*. Worcester, Birmingham.

[8] D. McGrew & J. Viega (2005). *The Galois/Counter Mode of Operation* (*GCM*). NIST, United State, US.

[9] National Institute of Standards and Technology (2001). *Advanced Encryption Standard* (*AES*). FIP 197, United State, US.

[10] National Institute of Standards and Technology (2002). *Secure Hash Standard* (*SHS*). FIPS 180-2, United State, US.

Appendix 1: Encryption Sate Array and Step by Step Matrices

State Array 0: Plaintext

00	10	20	30	40	50	60	70	80	90	A0	B0	C0	D0	E0	F0
01	11	21	31	41	51	61	71	81	91	A1	B1	C1	D1	E1	F1
02	12	22	32	42	52	62	72	82	92	A2	B2	C2	D2	E2	F2
03	13	23	33	43	53	63	73	83	93	A3	B3	C3	D3	E3	F3
04	14	24	34	44	54	64	74	84	94	A4	B4	C4	D4	E4	F4
05	15	25	35	45	55	65	75	85	95	A5	B5	C5	D5	E5	F5
06	16	26	36	46	56	66	76	86	96	A6	B6	C6	D6	E6	F6
07	17	27	37	47	57	67	77	87	97	A7	B7	C7	D7	E7	F7
08	18	28	38	48	58	68	78	88	98	A8	B8	C8	D8	E8	F8
09	19	29	39	49	59	69	79	89	99	A9	B9	C9	D9	E9	F9
0A	1A	2A	3A	4A	5A	6A	7A	8A	9A	AA	BA	CA	DA	EA	FA
0B	1B	2B	3B	4B	5B	6B	7B	8B	9B	AB	BB	CB	DB	EB	FB
0C	1C	2C	3C	4C	5C	6C	7C	8C	9C	AC	BC	CC	DC	EC	FC
0D	1D	2D	3D	4D	5D	6D	7D	8D	9D	AD	BD	CD	DD	ED	FD
0E	1E	2E	3E	4E	5E	6E	7E	8E	9E	AE	BE	CE	DE	EE	FE
0F	1F	2F	3F	4F	5F	6F	7F	8F	9F	AF	BF	CF	DF	EF	FF

Round Key 0

BA	78	16	BF	8F	01	CF	EA	41	41	40	DE	5D	AE	22	23
B0	03	61	A3	96	17	7A	9C	B4	10	FF	61	F2	00	15	AD
4F	8B	42	C2	2D	D3	72	9B	51	9B	A6	F6	8D	2D	A7	CC
5B	2D	60	6D	05	DA	ED	5A	D5	12	8C	C0	3E	6C	63	58
F2	A7	78	F1	A6	ED	3D	5B	C5	9A	5D	79	10	4C	59	8F
3F	07	09	3F	24	0C	A4	E9	13	33	FB	09	ED	4F	36	DA
EB	EA	18	7D	3D	64	EC	28	76	00	C6	BE	94	F0	DB	8A
B5	B5	FF	83	82	B6	AC	4A	45	21	8E	6E	5B	32	7C	7F
18	4F	6D	6E	82	55	4C	05	1B	33	F1	5E	7F	FF	FE	CB
0C	C0	F4	61	A2	90	96	C4	1C	21	4E	16	8E	34	C2	1D
31	3D	94	94	20	C4	C0	13	11	FC	FB	51	25	56	B9	D8
0C	46	FE	60	6F	47	F7	39	C6	58	E4	36	D0	33	B2	0C
34	AC	85	D4	5D	A1	E6	F4	CA	5E	61	B6	DC	C3	6E	F0
3A	BB	4D	2E	CA	BF	AA	B6	89	61	20	8D	45	88	35	3C
6E	55	CD	AE	2C	86	C0	1D	DC	30	CE	DD	0A	D0	4E	4E
9A	6A	7C	27	2D	AC	A6	2B	F4	19	26	67	8F	7E	75	04

State Array 1.0

BA	68	36	8F	CF	51	AF	9A	C1	D1	E0	6E	9D	7E	C2	D3
B1	12	40	92	D7	46	1B	ED	35	81	5E	D0	33	D1	F4	5C
4D	99	60	F0	6F	81	10	E9	D3	09	04	44	4F	FF	45	3E
58	3E	43	5E	46	89	8E	29	56	81	2F	73	FD	BF	80	AB
F6	B3	5C	C5	E2	B9	59	2F	41	0E	F9	CD	D4	98	BD	7B
3A	12	2C	0A	61	59	C1	9C	96	A6	5E	BC	28	9A	D3	2F
ED	FC	3E	4B	7B	32	8A	5E	F0	96	60	08	52	26	3D	7C
B2	A2	D8	B4	C5	E1	CB	3D	C2	B6	29	D9	9C	E5	9B	88
10	57	45	56	CA	0D	24	7D	93	AB	59	E6	B7	27	16	33
05	D9	DD	58	EB	C9	FF	BD	95	B8	E7	AF	47	ED	2B	E4
3B	27	BE	AE	6A	9E	AA	69	9B	66	51	EB	EF	8C	53	22
07	5D	D5	5B	24	1C	9C	42	4D	C3	4F	8D	1B	E8	59	F7
38	B0	A9	E8	11	FD	8A	88	46	C2	CD	0A	10	1F	82	0C
37	A6	60	13	87	E2	C7	CB	04	FC	8D	30	88	55	D8	C1
60	4B	E3	90	62	D8	AE	63	52	AE	60	63	C4	0E	A0	B0
95	75	53	18	62	F3	C9	54	7B	86	89	D8	40	A1	9A	FB

S-box Matrix S_I mod $m_I(x)$

63	2D	D6	59	2B	75	EC	B9	47	C9	FA	52	A4	7A	9C	72
7C	DD	02	06	45	08	96	07	89	9F	28	12	5A	AA	E3	F7
7E	87	AE	78	41	D9	D1	6C	70	E4	44	B8	0B	23	51	A9
8A	C1	30	09	D8	BF	5F	21	4C	A3	CF	C3	9D	BC	7B	A6
7F	3B	83	4D	85	CC	EE	E6	E0	95	3E	14	3A	18	76	BB
27	B2	D7	E1	5E	BA	AD	A2	84	5D	88	0A	F5	B6	62	34
97	5B	32	3F	CA	6A	C4	1B	BE	66	0D	FB	7D	DE	42	E9
73	2E	8D	D4	BD	4A	54	F2	2F	CE	FE	3C	B4	AC	61	4E
FF	17	4F	F3	13	24	74	64	82	37	26	6E	A5	AF	A1	B3
8F	55	16	58	49	F1	C6	F6	15	0F	6D	46	29	9E	B1	98
D3	1A	19	68	AB	A8	B0	D2	FD	4B	1D	60	04	01	11	9B
36	DB	71	93	69	77	3D	53	EF	05	80	00	EB	99	0E	90
8B	67	ED	48	CB	79	DF	C2	B7	03	E7	DA	22	C7	CD	F9
91	50	F4	25	33	40	A7	92	8C	1E	8E	B5	81	9A	6F	D5
6B	10	57	20	86	35	2A	56	0C	DC	65	31	F8	38	39	FC
A0	E5	EA	2C	1C	E2	F0	5C	43	C0	C5	D0	94	1F	E8	C8

State Array 1.1

60	74	3F	43	94	08	C5	4B	5A	AA	9C	2A	1E	56	0B	BC
12	87	2B	E4	AC	CA	DB	6F	E1	89	35	7A	09	AA	BB	79
33	0F	EC	72	F0	89	2D	B1	BC	8F	7F	85	1C	C8	5E	20
24	20	D8	35	CA	15	0C	16	6A	89	EA	21	D5	D0	47	80
E9	C3	79	F5	51	46	F1	EA	45	6B	98	81	18	37	B5	53
68	87	ED	D3	96	F1	5A	03	66	0D	35	DA	4F	4B	BC	EA
6F	F9	20	69	53	78	FD	35	72	66	EC	FF	D9	32	25	C2
B8	44	AF	14	F5	E3	EB	25	0B	FB	16	9E	03	62	05	82
2D	4A	5E	6A	04	91	83	92	A3	80	F1	42	3C	8D	5B	09
27	9E	9A	24	0E	29	C8	B5	5D	6E	61	C5	BD	6F	71	76
93	8D	31	65	B0	DC	1D	C6	05	C4	08	0E	E8	B7	BF	AE
73	40	B6	77	83	67	03	41	33	9D	1C	8C	DB	A1	F1	4E
F3	52	6D	A1	DD	D5	FD	82	CA	0B	81	D3	2D	E5	70	8B
D4	0D	EC	C1	2F	51	B4	EB	7F	F9	8C	59	82	BA	AF	5A
EC	69	7B	C9	D1	AF	65	5F	D9	65	EC	5F	3A	6B	FA	52
5D	A2	BF	17	D1	A6	29	CC	53	BE	15	AF	2B	28	4B	90

Mix Column Matrix M mod $m_1(x)$

03	02	01	01	01	01	01	01	01	01	01	01	01	01	01	01
02	03	02	01	01	01	01	01	01	01	01	01	01	01	01	01
01	02	03	02	01	01	01	01	01	01	01	01	01	01	01	01
01	01	02	03	02	01	01	01	01	01	01	01	01	01	01	01
01	01	01	02	03	02	01	01	01	01	01	01	01	01	01	01
01	01	01	01	02	03	02	01	01	01	01	01	01	01	01	01
01	01	01	01	01	02	03	02	01	01	01	01	01	01	01	01
01	01	01	01	01	01	02	03	02	01	01	01	01	01	01	01
01	01	01	01	01	01	01	02	03	02	01	01	01	01	01	01
01	01	01	01	01	01	01	01	02	03	02	01	01	01	01	01
01	01	01	01	01	01	01	01	01	02	03	02	01	01	01	01
01	01	01	01	01	01	01	01	01	01	02	03	02	01	01	01
01	01	01	01	01	01	01	01	01	01	01	02	03	02	01	01
01	01	01	01	01	01	01	01	01	01	01	01	02	03	02	01
01	01	01	01	01	01	01	01	01	01	01	01	01	02	03	02
01	01	01	01	01	01	01	01	01	01	01	01	01	01	02	03

State Array 1.2

B9	E2	3E	D8	74	99	35	07	7C	8F	57	6B	78	59	7A	C8
9E	00	35	E9	77	EB	5C	DB	28	16	7F	9F	4B	D6	28	6D
73	74	F0	E5	C9	8F	DA	E2	25	75	AF	7D	28	15	19	70
42	97	32	91	DF	AC	85	E1	34	7E	E6	FF	D2	81	12	AE
62	C7	90	99	EE	77	E1	E0	5E	31	4A	BE	EA	C8	ED	08
3E	C3	27	5B	A9	77	72	6C	55	4D	ED	AC	A9	B9	42	77
CA	1F	BB	E9	AB	3A	FB	20	93	BD	8D	A8	12	3F	20	07
D2	DE	CA	74	90	01	AD	A8	8E	9C	10	4A	5D	0E	02	49
9F	79	DE	DD	86	80	9A	B4	57	FF	4B	D8	CE	06	A0	35
E8	DD	93	00	43	79	E0	9D	BB	50	F9	C4	59	B0	6F	3E
BE	D0	2B	66	5F	BD	9E	B0	78	DD	8C	76	0E	1C	74	2F
09	62	9E	D0	32	29	DF	6E	DC	2B	93	CE	A6	BF	39	E3
40	DB	09	C1	E6	27	F1	DA	AB	FA	A9	68	EE	EC	88	11
ED	FF	F4	48	E2	D0	12	91	0B	2B	9F	BC	49	C6	4A	E4
0C	A0	3E	B1	08	BB	94	F7	2D	43	68	3E	FB	6B	52	C1
EA	7C	E5	07	79	41	2F	72	26	B8	2E	25	47	CD	39	ED

P-box Matrix P_1 mod $m_2(x)$

63	7C	AA	ED	C1	E6	24	88	32	3A	A1	3F	86	33	96	64
CB	E5	CF	14	44	45	0B	AC	D7	3C	4B	54	DF	A8	A6	80
37	B9	20	A5	73	BC	D8	5E	F0	1D	70	A9	11	0A	84	2D
7F	A2	8A	65	31	4E	F8	99	7B	D9	C0	09	81	29	92	FA
0F	EB	48	69	C2	41	00	DE	6B	B8	8C	8E	BE	BA	FD	4D
EC	BF	5C	A7	EA	9E	40	CC	1C	CA	91	62	D6	C4	02	78
2B	35	C5	AE	97	21	26	82	4A	F3	F5	36	E8	FE	1E	52
6F	59	3E	3B	B2	03	10	BB	12	2E	46	B6	9B	25	E9	27
55	A0	61	30	B0	98	66	DA	B3	D0	34	58	94	AB	FB	72
67	EF	C8	75	D2	2F	D3	17	8D	D4	C9	CE	2C	E7	74	43
A4	F4	0D	51	FC	A3	01	E2	E1	C3	DB	D1	B4	68	F2	5D
DC	F7	B7	16	1A	39	E3	6C	FF	3D	F6	13	95	50	EE	5A
47	2A	0E	1B	76	9A	85	57	5F	08	42	B5	87	90	93	7D
B1	79	6D	56	28	9F	8F	AF	E0	19	AD	D5	DD	C7	BD	71
23	6A	38	0C	8B	77	4F	7A	CD	7E	15	04	9C	18	49	E4
9D	05	83	53	F1	5B	89	C6	1F	F9	06	22	60	6E	07	4C

State Array 1.3

E1	9E	42	01	3E	7C	2E	39	FA	FF	15	5C	B1	2B	09	62
AD	28	8E	CE	E9	68	D0	9D	6B	2B	32	C1	55	75	20	26
F0	3A	25	0C	35	0E	FB	49	E2	81	DB	CA	59	70	9C	79
DD	DF	7C	59	4B	1F	A8	73	3E	29	8F	74	16	2B	CA	6B
72	77	A9	3E	77	EB	10	40	90	52	93	7F	ED	08	AC	94
BF	66	07	07	9F	9F	48	DA	D8	DE	E3	41	27	2F	E2	AB
47	DE	AC	B9	C8	91	9A	E8	1C	99	A0	5E	6E	F4	CD	D2
AF	E4	35	C9	6F	00	E6	BB	77	FF	F7	34	E2	11	43	42
6D	D2	20	E5	19	F1	78	EE	07	2F	32	08	4A	BB	BE	12
EC	ED	12	88	CE	A6	7A	AB	80	E1	27	5D	FB	EA	77	D0
79	57	97	BD	BE	E5	28	5B	D6	7D	3E	06	DB	9F	E9	91
86	ED	90	57	0E	68	4A	9E	31	74	C8	A8	8F	4A	EA	C3
E6	74	EE	DD	B9	BB	72	C6	93	F9	4D	9E	6C	2D	C4	35
FF	76	43	E0	50	BC	A9	28	DA	7E	B4	8C	09	49	E0	4B
0B	78	B0	DF	C1	00	99	B0	12	02	A9	C7	3E	D8	39	DD
25	79	74	BD	D0	8D	93	62	85	B8	AE	A0	5F	ED	3F	DC

Inverse Mix Column Matrix M^{-1} mod $m_2(x)$

2A	03	18	23	DF	4C	52	D5	31	0E	C0	BE	24	B6	05	80
03	64	22	3E	A5	9E	E2	44	FC	8A	A3	2E	F1	23	60	05
18	22	16	0B	E3	4E	A5	BA	8E	7C	21	70	86	73	23	B6
23	3E	0B	30	28	C9	6F	4A	1F	5C	BE	41	09	86	F1	24
DF	A5	E3	28	29	E3	A4	14	46	5F	D6	F4	41	70	2E	BE
4C	9E	4E	C9	E3	9D	29	45	B9	7D	CC	D6	BE	21	A3	C0
52	E2	A5	6F	A4	29	14	B0	4A	42	7D	5F	5C	7C	8A	0E
D5	44	BA	4A	14	45	B0	47	17	4A	B9	46	1F	8E	FC	31
31	FC	8E	1F	46	B9	4A	17	47	B0	45	14	4A	BA	44	D5
0E	8A	7C	5C	5F	7D	42	4A	B0	14	29	A4	6F	A5	E2	52
C0	A3	21	BE	D6	CC	7D	B9	45	29	9D	E3	C9	4E	9E	4C
BE	2E	70	41	F4	D6	5F	46	14	A4	E3	29	28	E3	A5	DF
24	F1	86	09	41	BE	5C	1F	4A	6F	C9	28	30	0B	3E	23
B6	23	73	86	70	21	7C	8E	BA	A5	4E	E3	0B	16	22	18
05	60	23	F1	2E	A3	8A	FC	44	E2	9E	A5	3E	22	64	03
80	05	B6	24	BE	C0	0E	31	D5	52	4C	DF	23	18	03	2A

State Array 1.4

14	CB	86	34	D5	58	9B	9E	40	04	1A	2E	CE	AB	5B	5D
B5	66	F8	A4	8B	EC	CE	38	AA	3D	F0	C8	90	DD	3D	DD
5B	09	6E	35	B2	60	AC	CB	29	5B	8E	29	A3	18	F0	89
B0	E0	58	05	43	CB	69	83	46	40	A2	BD	DB	EB	74	91
F7	62	DD	87	3B	4F	BC	16	0E	99	D8	1B	48	70	73	DB
03	DA	5E	A3	8E	85	42	A9	BE	F0	AC	87	4E	70	1A	2F
A7	87	43	0E	BD	A1	0B	55	DB	D6	6B	16	9F	F6	69	1D
C3	F4	7A	43	D2	9C	00	99	A4	73	A4	61	F5	8E	47	E2
B2	28	3E	7D	03	E1	6F	DC	B2	B1	11	8C	D9	CE	7A	0A
03	14	B9	00	15	10	91	90	F9	D8	8E	59	E3	65	29	75
D3	F5	DC	86	58	FE	54	9E	E0	DB	17	D4	8C	D8	31	89
44	D4	AB	D9	DD	4F	D7	43	42	C4	A4	0B	29	43	CD	61
EE	A8	5C	A6	06	04	CE	98	0F	1F	78	76	79	5F	7C	D6
95	63	6E	D5	7C	43	4B	2A	70	E9	20	ED	28	F1	44	B6
AF	93	DE	E3	AC	BA	28	77	50	EB	0E	B9	F0	05	0C	6B
61	37	A8	A1	39	F2	FF	DB	57	35	69	B6	E9	7C	C6	EF

Round Key 1

C6	C9	C6	F3	4A	20	4D	46	CC	25	64	E8	BF	D7	A8	E6
0B	FC	A1	AB	6D	84	CF	13	FF	EC	72	DD	DE	00	0D	A0
10	E2	86	F9	07	C0	FE	9F	02	CE	A3	86	4C	BA	EC	04
AE	47	E2	C0	A1	3B	60	47	3B	C9	96	8A	48	51	B2	19
97	AC	F4	3B	C0	A5	85	5E	68	48	DE	56	78	29	08	0F
F1	59	4E	18	31	EA	10	FF	02	B9	48	3A	7A	BD	7C	5F
AF	4B	F2	48	86	F5	02	95	10	75	92	CD	B6	38	81	E2
1C	F3	0E	28	F1	2C	99	7D	94	78	92	E5	1D	68	94	00
F9	94	AC	40	FF	A2	FF	D6	0A	78	95	19	84	9B	F9	CD
CC	9A	CE	CE	34	5C	46	16	B9	2E	F1	41	97	45	E7	B9
14	A8	62	5F	0F	F4	52	B3	09	36	57	70	F2	99	F8	62
E6	CF	05	14	70	06	5D	B7	0C	C2	41	9D	C6	F1	E6	A1
5C	4B	EB	16	E3	94	2C	22	A9	86	70	9D	AF	49	90	0D
4B	22	70	DF	FA	03	B5	C5	C6	A6	D0	8A	DE	DC	C2	6D
CE	C8	7E	29	35	8D	AC	43	13	91	84	E3	01	14	24	07
30	9A	C8	33	01	C7	39	08	34	AA	2F	9C	F2	45	B6	95

State Array 2.0

D2	02	40	C7	9F	78	D6	D8	8C	21	7E	C6	71	7C	F3	BB
BE	9A	59	0F	E6	68	01	2B	55	D1	82	15	4E	DD	30	7D
4B	EB	E8	CC	B5	A0	52	54	2B	95	2D	AF	EF	A2	1C	8D
1E	A7	BA	C5	E2	F0	09	C4	7D	89	34	37	93	BA	C6	88
60	CE	29	BC	FB	EA	39	48	66	D1	06	4D	30	59	7B	D4
F2	83	10	BB	BF	6F	52	56	BC	49	E4	BD	34	CD	66	70
08	CC	B1	46	3B	54	09	C0	CB	A3	F9	DB	29	CE	E8	FF
DF	07	74	6B	23	B0	99	E4	30	0B	36	84	E8	E6	D3	E2
4B	BC	92	3D	FC	43	90	0A	B8	C9	84	95	5D	55	83	C7
CF	8E	77	CE	21	4C	D7	86	40	F6	7F	18	74	20	CE	CC
C7	5D	BE	D9	57	0A	06	2D	E9	ED	40	A4	7E	41	C9	EB
A2	1B	AE	CD	AD	49	8A	F4	4E	06	E5	96	EF	B2	2B	C0
B2	E3	B7	B0	E5	90	E2	BA	A6	99	08	EB	D6	16	EC	DB
DE	41	1E	0A	86	40	FE	EF	B6	4F	F0	67	F6	2D	86	DB
61	5B	A0	CA	99	37	84	34	43	7A	8A	5A	F1	11	28	6C
51	AD	60	92	38	35	C6	D3	63	9F	46	2A	1B	39	70	7A

S-box Matrix S_2 mod $m_6(x)$

63	7C	D7	44	02	81	F0	F3	E8	13	12	24	91	74	10	C2
9D	2E	60	28	E0	F4	FB	6E	1A	DA	D3	61	E1	A1	B3	7F
27	45	FE	09	E2	C3	C6	0F	99	CE	A8	26	14	B0	DE	0A
E4	CF	BF	58	3B	A5	62	1C	19	B5	39	46	30	90	56	3C
7A	A9	70	35	AD	7B	6D	32	98	41	33	03	8A	52	55	C9
1E	D6	8E	F8	BD	A7	FA	88	D8	64	B1	6C	86	67	EC	21
A0	50	0E	53	0D	BA	C5	6A	4F	47	00	1D	E3	FD	DC	FC
65	BB	08	E5	4E	57	F1	FF	CA	48	9A	2A	F9	72	F7	84
EF	3E	3D	07	EA	2F	73	93	04	AF	6F	85	5F	76	CB	23
9E	1F	49	D4	4B	CC	68	69	97	17	C0	A3	78	D1	36	A2
DD	D9	82	8D	AE	8C	95	3F	0C	9B	01	4A	94	8B	96	06
BE	16	DB	BC	31	92	DF	C4	AA	89	5A	80	A4	B6	42	C8
B9	F6	C1	25	D5	51	40	77	54	7E	B4	9C	0B	1B	E7	6B
75	05	71	D0	E9	2B	5C	5E	18	D2	2C	7D	87	43	AC	37
5B	5D	34	A6	ED	83	20	4D	F5	8F	79	4C	11	66	2D	E6
B7	59	CD	22	9F	38	C7	B2	15	3A	EB	EE	29	B8	AB	F2

State Array 2.1

71	D7	7A	77	A2	CA	5C	18	5F	45	F7	40	BB	F9	22	80
42	C0	64	C2	20	4F	7C	26	A7	05	3D	F4	55	43	E4	72
03	4C	F5	0B	92	DD	8E	BD	26	CC	B0	06	E6	82	E1	76
B3	3F	5A	51	34	B7	13	D5	72	AF	3B	1C	D4	5A	40	04
A0	E7	CE	A4	EE	79	B5	98	C5	05	F0	52	E4	64	2A	E9
CD	07	9D	80	C8	FC	8E	FA	A4	41	ED	B6	3B	1B	C5	65
E8	0B	16	6D	46	BD	13	B9	9C	8D	3A	7D	CE	E7	F5	F2
37	F3	4E	1D	09	BE	17	ED	E4	24	62	EA	F5	20	D0	34
03	A4	49	90	29	35	9E	12	AA	7E	EA	CC	67	A7	07	77
6B	CB	FF	E7	45	8A	5E	73	7A	C7	84	1A	4E	27	E7	0B
77	67	42	D2	88	12	F0	B0	8F	66	7A	AE	F7	A9	7E	4C
82	61	96	1B	8B	41	6F	9F	55	F0	83	68	E6	DB	26	B9
DB	A6	C4	BE	83	9E	34	5A	95	17	E8	4C	5C	FB	11	7D
AC	A9	B3	12	73	7A	AB	E6	DF	C9	B7	6A	C7	B0	73	7D
50	6C	DD	B4	17	1C	EA	3B	35	9A	6F	B1	59	2E	99	E3
D6	8B	A0	49	19	A5	40	D0	53	A2	6D	A8	61	B5	65	9A

Inverse Mix Column Matrix M^{-1} mod $m_6(x)$

50	4D	B5	B9	49	E5	DD	E0	4F	B8	0C	23	1C	19	20	0B
4D	FE	6E	83	A5	CD	1A	E8	22	5C	C2	E9	45	A6	09	20
B5	6E	49	16	E5	18	FC	B9	9A	5C	FB	46	37	D4	A6	19
B9	83	16	CA	C8	17	3E	6E	27	B8	1B	46	32	37	45	1C
49	A5	E5	C8	BE	C8	E5	A5	49	00	23	E9	46	46	E9	23
E5	CD	18	17	C8	EC	B5	41	01	34	52	23	1B	FB	C2	0C
DD	1A	FC	3E	E5	B5	0E	32	1F	15	34	00	B8	5C	5C	B8
E0	E8	B9	6E	A5	41	32	35	43	1F	01	49	27	9A	22	4F
4F	22	9A	27	49	01	1F	43	35	32	41	A5	6E	B9	E8	E0
B8	5C	5C	B8	00	34	15	1F	32	0E	B5	E5	3E	FC	1A	DD
0C	C2	FB	1B	23	52	34	01	41	B5	EC	C8	17	18	CD	E5
23	E9	46	46	E9	23	00	49	A5	E5	C8	BE	C8	E5	A5	49
1C	45	37	32	46	1B	B8	27	6E	3E	17	C8	CA	16	83	B9
19	A6	D4	37	46	FB	5C	9A	B9	FC	18	E5	16	49	6E	B5
20	09	A6	45	E9	C2	5C	22	E8	1A	CD	A5	83	6E	FE	4D
0B	20	19	1C	23	0C	B8	4F	E0	DD	E5	49	B9	B5	4D	50

State Array 2.2

8E	9F	CE	6B	ED	DC	30	E9	80	65	99	C8	49	DD	CA	F0
98	BB	96	22	93	AF	5F	A2	AC	D5	C1	3E	B8	62	C8	54
A2	11	83	54	54	52	84	92	4C	50	CF	3E	B4	03	FD	32
A7	3C	B2	BF	7F	F9	96	31	1E	E0	59	27	9D	BD	DA	6F
4A	30	5D	4D	E8	51	9B	5A	AE	25	CA	3F	B1	40	0B	F0
49	5D	AA	E8	6F	70	5C	31	F0	75	46	0C	01	42	94	1C
3C	47	6F	C0	A1	24	C2	36	0B	EC	97	6A	B8	96	4B	4F
7A	83	67	0E	69	E3	9A	66	EF	16	C8	E5	34	58	EF	0D
3E	49	9A	82	12	8D	68	8C	84	44	FA	04	6C	45	EB	60
AD	8D	39	7E	29	C6	EB	84	A9	55	40	96	FE	E0	BB	55
92	5B	D5	77	E5	0E	1A	41	05	CF	84	D9	5D	FA	3E	8B
9E	DE	14	96	AC	BD	5D	8E	B3	EC	EC	EC	DB	88	5E	17
FA	4D	8B	66	AE	27	A3	65	8D	87	8E	C7	32	E0	12	72
38	D6	2F	44	E3	8C	79	5B	EE	0A	83	DC	6C	C2	17	55
4C	13	E4	EC	C7	39	DF	F0	15	DD	63	46	98	AF	C2	0A
82	4D	E8	DD	2F	D7	FE	F6	82	FB	27	F8	14	B1	07	8C

P-box Matrix P_2 mod $m_7(x)$

63	7C	18	31	2A	0A	4A	FA	C7	EB	23	AD	03	3A	5B	BB
C5	D4	D3	E8	43	50	04	54	A7	1D	CF	1B	8B	7E	FB	F9
C4	EA	4C	85	3B	86	52	97	87	FD	0E	B6	D0	4B	F8	1C
01	F2	5C	F1	C1	1A	AB	6B	17	D6	19	14	DB	9F	DA	8D
44	C6	53	A1	F4	9B	E4	37	4F	EE	65	57	0F	4E	ED	71
E5	21	2C	B4	D5	B5	89	C9	BA	3C	83	69	5A	CD	DC	EC
A6	26	5F	BC	FC	99	DE	12	32	68	2B	60	F3	EF	67	98
59	11	4D	DD	AA	29	D8	84	3F	10	E9	B1	BF	77	E0	82
F0	C3	45	CE	8F	90	F6	6F	A8	06	1F	15	A0	2D	BD	AF
75	B8	A5	B2	94	09	79	A3	55	3E	F5	80	24	E3	6A	02
20	51	42	07	30	8E	88	C2	CC	B3	08	96	16	61	36	CA
7B	6D	38	22	13	FF	66	40	0B	B7	C0	3D	48	62	A4	D9
81	7F	35	00	7D	7A	8C	9C	AC	F7	1E	6E	49	A2	2F	6C
CB	92	E6	28	47	39	E2	78	DF	27	25	E7	95	D7	9E	34
8A	41	AE	70	74	33	C8	5E	73	91	46	A9	BE	9A	64	E1
B9	58	2E	5D	D2	D1	FE	72	0D	05	9D	0C	56	B0	93	76

State Array 2.3

66	A7	55	49	5F	FB	44	77	84	C6	DC	B3	F8	82	CF	B1
16	83	36	AC	27	04	5D	1E	CE	59	F9	3E	32	D5	8E	FA
92	5D	96	99	FE	83	47	0A	44	E3	ED	97	AA	45	E8	12
E5	6B	0B	39	55	8B	3E	5A	14	8C	DD	54	75	EC	55	EF
8E	13	D5	93	4A	9A	63	E3	DB	32	30	03	83	67	40	AE
AF	5B	84	5D	A2	A9	14	3F	4D	7A	01	CA	B2	DD	F0	6F
6A	FA	88	8E	C2	CA	5D	4B	EC	0C	BB	31	72	DE	C7	8C
EC	F0	F6	15	C7	AD	8C	58	5B	EB	27	9E	9F	AE	62	4D
96	FA	0D	46	66	54	52	4C	1A	5C	4C	B8	A3	6F	0E	12
8D	DD	D6	07	29	6C	D9	92	4F	24	AF	51	65	27	17	BD
6C	4D	E0	84	5E	39	3C	AC	84	46	69	96	8D	C8	E4	60
B1	E5	7E	CF	E8	70	3E	EC	8D	82	F0	F0	C0	EB	98	34
EC	7F	41	49	A2	98	30	80	DF	31	8B	38	05	42	82	C1
B4	D7	2F	96	BB	6F	E0	C2	9A	17	DA	9D	94	0E	C2	EE
EF	0A	79	E0	9B	49	2F	DC	22	C8	11	65	1C	0B	25	96
3E	BF	3C	B8	E8	40	68	87	FD	54	E9	C8	A1	50	FE	BD

Mix Column Matrix M mod $m_7(x)$

03	02	01	01	01	01	01	01	01	01	01	01	01	01	01	01
02	03	02	01	01	01	01	01	01	01	01	01	01	01	01	01
01	02	03	02	01	01	01	01	01	01	01	01	01	01	01	01
01	01	02	03	02	01	01	01	01	01	01	01	01	01	01	01
01	01	01	02	03	02	01	01	01	01	01	01	01	01	01	01
01	01	01	01	02	03	02	01	01	01	01	01	01	01	01	01
01	01	01	01	01	02	03	02	01	01	01	01	01	01	01	01
01	01	01	01	01	01	02	03	02	01	01	01	01	01	01	01
01	01	01	01	01	01	01	02	03	02	01	01	01	01	01	01
01	01	01	01	01	01	01	01	02	03	02	01	01	01	01	01
01	01	01	01	01	01	01	01	01	02	03	02	01	01	01	01
01	01	01	01	01	01	01	01	01	01	02	03	02	01	01	01
01	01	01	01	01	01	01	01	01	01	01	02	03	02	01	01
01	01	01	01	01	01	01	01	01	01	01	01	02	03	02	01
01	01	01	01	01	01	01	01	01	01	01	01	01	02	03	02
01	01	01	01	01	01	01	01	01	01	01	01	01	01	02	03

State Array 2.4

19	09	4F	1C	7A	31	B7	BD	A7	D9	D8	6C	2F	33	1B	25
38	CA	71	B5	E7	AC	67	CA	21	84	2D	BF	FC	AB	85	58
DE	A7	33	10	20	BB	F3	A9	FC	E0	3A	D8	14	89	AA	52
E6	C6	6C	F1	3C	F6	C8	19	93	32	B6	5C	FF	11	A2	53
CA	B4	84	F0	C7	99	60	FF	47	C0	88	EC	21	D5	9F	95
9D	A8	B7	00	71	69	B2	10	3E	EF	13	8A	19	39	7E	F1
FE	CB	DE	BE	61	53	2D	4E	F8	15	90	31	FD	86	2F	D0
33	C5	DC	08	CF	D4	36	C8	B6	98	DB	08	23	C7	6F	96
87	A6	C5	27	B4	20	83	50	F5	57	8C	8E	26	EA	94	9A
FB	A1	24	32	B7	43	3F	75	26	3F	BD	7F	D6	08	E0	42
73	10	87	CD	B5	7A	6E	4C	B3	D8	58	60	9B	8C	4E	F5
0D	B9	47	54	79	C8	B0	3A	ED	23	AD	BD	76	00	6A	25
DF	6A	CE	E4	FB	DA	3D	E4	9D	63	E4	68	98	04	1A	A5
65	14	A9	4A	77	66	DE	F6	CE	9B	71	95	8A	8F	7A	8B
AF	6E	78	C8	89	CF	F9	E1	10	EB	1C	9A	09	BC	19	77
45	45	4C	CD	D0	77	79	1B	86	4E	6D	77	EF	F5	63	89

Round Key 2

2C	10	7E	D3	18	2F	C4	6D	C5	0A	2B	4C	89	B6	6B	57
D7	0D	D7	FD	97	FE	45	7E	61	1D	A2	19	B3	5C	85	B6
10	50	80	8F	15	0E	97	6D	7F	B0	31	58	2C	04	39	56
75	C5	2E	FA	75	6C	D9	50	37	90	E5	9A	F0	AB	42	01
2A	17	DD	62	EB	0D	BA	17	1D	8F	DE	93	A8	5C	3A	6A
9A	2C	A0	6A	A1	37	72	ED	D3	9C	6F	1A	B2	B3	FB	70
EE	34	24	C7	8E	66	61	72	91	A9	CE	E6	59	BB	79	45
98	8B	2B	75	A4	BF	1F	B7	B8	1A	CD	E5	C8	0C	51	49
F9	ED	12	6A	E2	DC	BD	09	A0	C6	F5	E9	E1	77	F0	8F
2B	67	D2	E5	69	4E	61	EB	01	C8	2F	CA	1F	02	C3	36
5D	EC	C8	BB	99	82	AD	DD	18	6B	D1	74	8F	F1	D6	2A
24	F0	66	D9	75	45	9D	5B	DA	6E	AB	E4	CD	3C	48	8B
97	B3	57	D5	18	F8	D6	32	34	5B	75	DC	6B	D1	C7	2C
FD	B1	A9	60	34	20	C3	BB	A1	A6	72	7A	E8	BF	B5	E7
2C	68	5C	5F	DF	5E	2E	CE	65	8A	C7	59	DD	AE	DD	8F
68	40	B6	40	BE	12	81	08	65	CB	51	24	B8	C5	ED	EA

State Array 3: Ciphertext

35	19	31	CF	62	1E	73	D0	62	D3	F3	20	A6	85	70	72
EF	C7	A6	48	70	52	22	B4	40	99	8F	A6	4F	F7	00	EE
CE	F7	B3	9F	35	B5	64	C4	83	50	0B	80	38	8D	93	04
93	03	42	0B	49	9A	11	49	A4	A2	53	C6	0F	BA	E0	52
E0	A3	59	92	2C	94	DA	E8	5A	4F	56	7F	89	89	A5	FF
07	84	17	6A	D0	5E	C0	FD	ED	73	7C	90	AB	8A	85	81
10	FF	FA	79	EF	35	4C	3C	69	BC	5E	D7	A4	3D	56	95
AB	4E	F7	7D	6B	6B	29	7F	0E	82	16	ED	EB	CB	3E	DF
7E	4B	D7	4D	56	FC	3E	59	55	91	79	67	C7	9D	64	15
D0	C6	F6	D7	DE	0D	5E	9E	27	F7	92	B5	C9	0A	23	74
2E	FC	4F	76	2C	F8	C3	91	AB	B3	89	14	14	7D	98	DF
29	49	21	8D	0C	8D	2D	61	37	4D	06	59	BB	3C	22	AE
48	D9	99	31	E3	22	EB	D6	A9	38	91	B4	F3	D5	DD	89
98	A5	00	2A	43	46	1D	4D	6F	3D	03	EF	62	30	CF	6C
83	06	24	97	56	91	D7	2F	75	61	DB	C3	D4	12	C4	F8
2D	05	FA	8D	6E	65	F8	13	E3	85	3C	53	57	30	8E	63

Appendix 2: Decryption Sate Array and Step by Step Matrices

State Array 0: Ciphertext

35	19	31	CF	62	1E	73	D0	62	D3	F3	20	A6	85	70	72
EF	C7	A6	48	70	52	22	B4	40	99	8F	A6	4F	F7	00	EE
CE	F7	B3	9F	35	B5	64	C4	83	50	0B	80	38	8D	93	04
93	03	42	0B	49	9A	11	49	A4	A2	53	C6	0F	BA	E0	52
E0	A3	59	92	2C	94	DA	E8	5A	4F	56	7F	89	89	A5	FF
07	84	17	6A	D0	5E	C0	FD	ED	73	7C	90	AB	8A	85	81
10	FF	FA	79	EF	35	4C	3C	69	BC	5E	D7	A4	3D	56	95
AB	4E	F7	7D	6B	6B	29	7F	0E	82	16	ED	EB	CB	3E	DF
7E	4B	D7	4D	56	FC	3E	59	55	91	79	67	C7	9D	64	15
D0	C6	F6	D7	DE	0D	5E	9E	27	F7	92	B5	C9	0A	23	74
2E	FC	4F	76	2C	F8	C3	91	AB	B3	89	14	14	7D	98	DF
29	49	21	8D	0C	8D	2D	61	37	4D	06	59	BB	3C	22	AE
48	D9	99	31	E3	22	EB	D6	A9	38	91	B4	F3	D5	DD	89
98	A5	00	2A	43	46	1D	4D	6F	3D	03	EF	62	30	CF	6C
83	06	24	97	56	91	D7	2F	75	61	DB	C3	D4	12	C4	F8
2D	05	FA	8D	6E	65	F8	13	E3	85	3C	53	57	30	8E	63

Round Key 2

2C	10	7E	D3	18	2F	C4	6D	C5	0A	2B	4C	89	B6	6B	57
D7	0D	D7	FD	97	FE	45	7E	61	1D	A2	19	B3	5C	85	B6
10	50	80	8F	15	0E	97	6D	7F	B0	31	58	2C	04	39	56
75	C5	2E	FA	75	6C	D9	50	37	90	E5	9A	F0	AB	42	01
2A	17	DD	62	EB	0D	BA	17	1D	8F	DE	93	A8	5C	3A	6A
9A	2C	A0	6A	A1	37	72	ED	D3	9C	6F	1A	B2	B3	FB	70
EE	34	24	C7	8E	66	61	72	91	A9	CE	E6	59	BB	79	45
98	8B	2B	75	A4	BF	1F	B7	B8	1A	CD	E5	C8	0C	51	49
F9	ED	12	6A	E2	DC	BD	09	A0	C6	F5	E9	E1	77	F0	8F
2B	67	D2	E5	69	4E	61	EB	01	C8	2F	CA	1F	02	C3	36
5D	EC	C8	BB	99	82	AD	DD	18	6B	D1	74	8F	F1	D6	2A
24	F0	66	D9	75	45	9D	5B	DA	6E	AB	E4	CD	3C	48	8B
97	B3	57	D5	18	F8	D6	32	34	5B	75	DC	6B	D1	C7	2C
FD	B1	A9	60	34	20	C3	BB	A1	A6	72	7A	E8	BF	B5	E7
2C	68	5C	5F	DF	5E	2E	CE	65	8A	C7	59	DD	AE	DD	8F
68	40	B6	40	BE	12	81	08	65	CB	51	24	B8	C5	ED	EA

State Array 1.0

19	09	4F	1C	7A	31	B7	BD	A7	D9	D8	6C	2F	33	1B	25
38	CA	71	B5	E7	AC	67	CA	21	84	2D	BF	FC	AB	85	58
DE	A7	33	10	20	BB	F3	A9	FC	E0	3A	D8	14	89	AA	52
E6	C6	6C	F1	3C	F6	C8	19	93	32	B6	5C	FF	11	A2	53
CA	B4	84	F0	C7	99	60	FF	47	C0	88	EC	21	D5	9F	95
9D	A8	B7	00	71	69	B2	10	3E	EF	13	8A	19	39	7E	F1
FE	CB	DE	BE	61	53	2D	4E	F8	15	90	31	FD	86	2F	D0
33	C5	DC	08	CF	D4	36	C8	B6	98	DB	08	23	C7	6F	96
87	A6	C5	27	B4	20	83	50	F5	57	8C	8E	26	EA	94	9A
FB	A1	24	32	B7	43	3F	75	26	3F	BD	7F	D6	08	E0	42
73	10	87	CD	B5	7A	6E	4C	B3	D8	58	60	9B	8C	4E	F5
0D	B9	47	54	79	C8	B0	3A	ED	23	AD	BD	76	00	6A	25
DF	6A	CE	E4	FB	DA	3D	E4	9D	63	E4	68	98	04	1A	A5
65	14	A9	4A	77	66	DE	F6	CE	9B	71	95	8A	8F	7A	8B
AF	6E	78	C8	89	CF	F9	E1	10	EB	1C	9A	09	BC	19	77
45	45	4C	CD	D0	77	79	1B	86	4E	6D	77	EF	F5	63	89

Inverse Mix Column Matrix M^{-1} mod $m_7(x)$

3A	35	A7	E9	0F	58	79	10	7F	5C	AC	2F	80	C9	B5	09
35	37	01	85	4B	E6	43	28	62	D8	E3	D6	CB	E8	6A	B5
A7	01	62	24	3C	6A	16	B5	0B	7C	98	57	39	1F	E8	C9
E9	85	24	2B	22	81	4A	C6	58	9D	85	50	73	39	CB	80
0F	4B	3C	22	41	BF	77	A4	53	87	E8	76	50	57	D6	2F
58	E6	6A	81	BF	DD	A0	36	AF	D7	1E	E8	85	98	E3	AC
79	43	16	4A	77	A0	07	15	0C	AD	D7	87	9D	7C	D8	5C
10	28	B5	C6	A4	36	15	18	32	0C	AF	53	58	0B	62	7F
7F	62	0B	58	53	AF	0C	32	18	15	36	A4	C6	B5	28	10
5C	D8	7C	9D	87	D7	AD	0C	15	07	A0	77	4A	16	43	79
AC	E3	98	85	E8	1E	D7	AF	36	A0	DD	BF	81	6A	E6	58
2F	D6	57	50	76	E8	87	53	A4	77	BF	41	22	3C	4B	0F
80	CB	39	73	50	85	9D	58	C6	4A	81	22	2B	24	85	E9
C9	E8	1F	39	57	98	7C	0B	B5	16	6A	3C	24	62	01	A7
B5	6A	E8	CB	D6	E3	D8	62	28	43	E6	4B	85	01	37	35
09	B5	C9	80	2F	AC	5C	7F	10	79	58	0F	E9	A7	35	3A

State Array 1.1

66	A7	55	49	5F	FB	44	77	84	C6	DC	B3	F8	82	CF	B1
16	83	36	AC	27	04	5D	1E	CE	59	F9	3E	32	D5	8E	FA
92	5D	96	99	FE	83	47	0A	44	E3	ED	97	AA	45	E8	12
E5	6B	0B	39	55	8B	3E	5A	14	8C	DD	54	75	EC	55	EF
8E	13	D5	93	4A	9A	63	E3	DB	32	30	03	83	67	40	AE
AF	5B	84	5D	A2	A9	14	3F	4D	7A	01	CA	B2	DD	F0	6F
6A	FA	88	8E	C2	CA	5D	4B	EC	0C	BB	31	72	DE	C7	8C
EC	F0	F6	15	C7	AD	8C	58	5B	EB	27	9E	9F	AE	62	4D
96	FA	0D	46	66	54	52	4C	1A	5C	4C	B8	A3	6F	0E	12
8D	DD	D6	07	29	6C	D9	92	4F	24	AF	51	65	27	17	BD
6C	4D	E0	84	5E	39	3C	AC	84	46	69	96	8D	C8	E4	60
B1	E5	7E	CF	E8	70	3E	EC	8D	82	F0	F0	C0	EB	98	34
EC	7F	41	49	A2	98	30	80	DF	31	8B	38	05	42	82	C1
B4	D7	2F	96	BB	6F	E0	C2	9A	17	DA	9D	94	0E	C2	EE
EF	0A	79	E0	9B	49	2F	DC	22	C8	11	65	1C	0B	25	96
3E	BF	3C	B8	E8	40	68	87	FD	54	E9	C8	A1	50	FE	BD

Inverse P-box Matrix P_2^{-1} mod $m_7(x)$

C3	79	A0	A4	B7	15	6B	E3	9B	85	8C	FD	BA	2C	7E	80
30	71	51	03	E1	A1	AD	4F	C0	E9	43	7B	34	F5	EF	33
9F	67	B3	68	A2	26	BD	F7	7F	D1	CD	93	A7	F4	D6	31
0C	B4	0A	E5	14	42	00	E8	5A	FE	97	A9	81	12	9D	6C
16	3B	9C	DF	40	17	EE	E4	77	94	BE	53	20	11	46	44
F9	8B	DA	C2	82	98	4A	90	23	DC	92	55	10	54	50	9A
89	AC	61	AE	EA	FC	B6	FF	25	AB	60	2B	41	39	D2	86
A3	38	D9	47	D4	4B	6E	7D	28	27	18	B9	08	DD	DB	C9
AA	02	D3	B2	BC	F1	69	D7	A6	6F	88	91	E6	76	13	2E
95	3A	75	D5	CC	70	5B	96	56	65	EB	F0	57	BF	7A	1F
05	35	04	0D	06	5C	9E	C5	E0	ED	74	58	AF	3E	21	07
B8	1B	6A	24	2D	0E	37	B0	1C	45	36	0F	D0	3C	09	1E
FB	2F	52	59	22	32	CF	01	C6	C7	C8	63	A8	5E	5F	64
F8	19	8D	BB	72	F3	B1	C4	3F	FA	0B	8E	5D	73	4E	29
2A	CA	F2	99	4D	E7	CB	1D	A5	DE	E2	EC	83	66	49	F6
4C	8A	CE	78	48	62	87	C1	84	3D	8F	7C	1A	D8	6D	B5

State Array 1.2

8E	9F	CE	6B	ED	DC	30	E9	80	65	99	C8	49	DD	CA	F0
98	BB	96	22	93	AF	5F	A2	AC	D5	C1	3E	B8	62	C8	54
A2	11	83	54	54	52	84	92	4C	50	CF	3E	B4	03	FD	32
A7	3C	B2	BF	7F	F9	96	31	1E	E0	59	27	9D	BD	DA	6F
4A	30	5D	4D	E8	51	9B	5A	AE	25	CA	3F	B1	40	0B	F0
49	5D	AA	E8	6F	70	5C	31	F0	75	46	0C	01	42	94	1C
3C	47	6F	C0	A1	24	C2	36	0B	EC	97	6A	B8	96	4B	4F
7A	83	67	0E	69	E3	9A	66	EF	16	C8	E5	34	58	EF	0D
3E	49	9A	82	12	8D	68	8C	84	44	FA	04	6C	45	EB	60
AD	8D	39	7E	29	C6	EB	84	A9	55	40	96	FE	E0	BB	55
92	5B	D5	77	E5	0E	1A	41	05	CF	84	D9	5D	FA	3E	8B
9E	DE	14	96	AC	BD	5D	8E	B3	EC	EC	EC	DB	88	5E	17
FA	4D	8B	66	AE	27	A3	65	8D	87	8E	C7	32	E0	12	72
38	D6	2F	44	E3	8C	79	5B	EE	0A	83	DC	6C	C2	17	55
4C	13	E4	EC	C7	39	DF	F0	15	DD	63	46	98	AF	C2	0A
82	4D	E8	DD	2F	D7	FE	F6	82	FB	27	F8	14	B1	07	8C

Mix Column Matrix M mod $m_6(x)$

03	02	01	01	01	01	01	01	01	01	01	01	01	01	01	01
02	03	02	01	01	01	01	01	01	01	01	01	01	01	01	01
01	02	03	02	01	01	01	01	01	01	01	01	01	01	01	01
01	01	02	03	02	01	01	01	01	01	01	01	01	01	01	01
01	01	01	02	03	02	01	01	01	01	01	01	01	01	01	01
01	01	01	01	02	03	02	01	01	01	01	01	01	01	01	01
01	01	01	01	01	02	03	02	01	01	01	01	01	01	01	01
01	01	01	01	01	01	02	03	02	01	01	01	01	01	01	01
01	01	01	01	01	01	01	02	03	02	01	01	01	01	01	01
01	01	01	01	01	01	01	01	02	03	02	01	01	01	01	01
01	01	01	01	01	01	01	01	01	02	03	02	01	01	01	01
01	01	01	01	01	01	01	01	01	01	02	03	02	01	01	01
01	01	01	01	01	01	01	01	01	01	01	02	03	02	01	01
01	01	01	01	01	01	01	01	01	01	01	01	02	03	02	01
01	01	01	01	01	01	01	01	01	01	01	01	01	02	03	02
01	01	01	01	01	01	01	01	01	01	01	01	01	01	02	03

State Array 1.3

71	D7	7A	77	A2	CA	5C	18	5F	45	F7	40	BB	F9	22	80
42	C0	64	C2	20	4F	7C	26	A7	05	3D	F4	55	43	E4	72
03	4C	F5	0B	92	DD	8E	BD	26	CC	B0	06	E6	82	E1	76
B3	3F	5A	51	34	B7	13	D5	72	AF	3B	1C	D4	5A	40	04
A0	E7	CE	A4	EE	79	B5	98	C5	05	F0	52	E4	64	2A	E9
CD	07	9D	80	C8	FC	8E	FA	A4	41	ED	B6	3B	1B	C5	65
E8	0B	16	6D	46	BD	13	B9	9C	8D	3A	7D	CE	E7	F5	F2
37	F3	4E	1D	09	BE	17	ED	E4	24	62	EA	F5	20	D0	34
03	A4	49	90	29	35	9E	12	AA	7E	EA	CC	67	A7	07	77
6B	CB	FF	E7	45	8A	5E	73	7A	C7	84	1A	4E	27	E7	0B
77	67	42	D2	88	12	F0	B0	8F	66	7A	AE	F7	A9	7E	4C
82	61	96	1B	8B	41	6F	9F	55	F0	83	68	E6	DB	26	B9
DB	A6	C4	BE	83	9E	34	5A	95	17	E8	4C	5C	FB	11	7D
AC	A9	B3	12	73	7A	AB	E6	DF	C9	B7	6A	C7	B0	73	7D
50	6C	DD	B4	17	1C	EA	3B	35	9A	6F	B1	59	2E	99	E3
D6	8B	A0	49	19	A5	40	D0	53	A2	6D	A8	61	B5	65	9A

Inverse S-box Matrix S_2^{-1} mod $m_6(x)$

6A	0E	E6	3C	C6	61	12	42	BB	3D	60	2D	9A	D3	14	06
AA	EC	5F	B4	49	C5	1B	D2	05	0C	1D	5A	C2	9D	1C	76
04	0A	F3	47	BE	4D	36	7D	A2	B5	9F	F7	0F	D9	24	FF
4B	09	8F	4A	DD	63	00	86	E5	87	9B	1E	25	1A	6C	07
88	2C	0B	E2	03	C8	59	0D	7F	AC	BC	CA	B7	93	30	15
D1	F8	C3	43	21	4E	70	D0	8B	A6	35	39	66	C4	73	E8
AF	B1	2B	9E	3B	3E	ED	8D	5C	AE	E3	BD	26	51	EF	C1
83	99	20	DF	69	75	5D	C7	DC	98	55	F0	F6	02	CE	7E
72	D8	13	F5	79	33	96	9C	57	48	2A	FD	BF	58	08	53
23	38	FC	3A	92	F1	97	EA	B9	28	41	C0	4F	A1	D4	7C
2F	18	7B	F9	AB	BA	67	40	4C	7A	B8	65	78	19	84	56
CC	CD	D5	34	94	E0	CF	45	AD	A9	FE	71	8E	B2	FA	16
A8	37	DA	3F	EB	D6	5B	01	A5	CB	DE	B3	95	6E	5E	6F
64	6B	EE	82	E7	E1	46	DB	A3	10	44	54	F2	A0	E4	6D
62	50	11	81	74	D7	17	C9	52	90	A4	B0	29	2E	FB	22
27	91	85	A7	68	8C	8A	1F	E9	F4	89	32	31	B6	80	77

State Array 1.4

D2	02	40	C7	9F	78	D6	D8	8C	21	7E	C6	71	7C	F3	BB
BE	9A	59	0F	E6	68	01	2B	55	D1	82	15	4E	DD	30	7D
4B	EB	E8	CC	B5	A0	52	54	2B	95	2D	AF	EF	A2	1C	8D
1E	A7	BA	C5	E2	F0	09	C4	7D	89	34	37	93	BA	C6	88
60	CE	29	BC	FB	EA	39	48	66	D1	06	4D	30	59	7B	D4
F2	83	10	BB	BF	6F	52	56	BC	49	E4	BD	34	CD	66	70
08	CC	B1	46	3B	54	09	C0	CB	A3	F9	DB	29	CE	E8	FF
DF	07	74	6B	23	B0	99	E4	30	0B	36	84	E8	E6	D3	E2
4B	BC	92	3D	FC	43	90	0A	B8	C9	84	95	5D	55	83	C7
CF	8E	77	CE	21	4C	D7	86	40	F6	7F	18	74	20	CE	CC
C7	5D	BE	D9	57	0A	06	2D	E9	ED	40	A4	7E	41	C9	EB
A2	1B	AE	CD	AD	49	8A	F4	4E	06	E5	96	EF	B2	2B	C0
B2	E3	B7	B0	E5	90	E2	BA	A6	99	08	EB	D6	16	EC	DB
DE	41	1E	0A	86	40	FE	EF	B6	4F	F0	67	F6	2D	86	DB
61	5B	A0	CA	99	37	84	34	43	7A	8A	5A	F1	11	28	6C
51	AD	60	92	38	35	C6	D3	63	9F	46	2A	1B	39	70	7A

Round Key 1

C6	C9	C6	F3	4A	20	4D	46	CC	25	64	E8	BF	D7	A8	E6
0B	FC	A1	AB	6D	84	CF	13	FF	EC	72	DD	DE	00	0D	A0
10	E2	86	F9	07	C0	FE	9F	02	CE	A3	86	4C	BA	EC	04
AE	47	E2	C0	A1	3B	60	47	3B	C9	96	8A	48	51	B2	19
97	AC	F4	3B	C0	A5	85	5E	68	48	DE	56	78	29	08	0F
F1	59	4E	18	31	EA	10	FF	02	B9	48	3A	7A	BD	7C	5F
AF	4B	F2	48	86	F5	02	95	10	75	92	CD	B6	38	81	E2
1C	F3	0E	28	F1	2C	99	7D	94	78	92	E5	1D	68	94	00
F9	94	AC	40	FF	A2	FF	D6	0A	78	95	19	84	9B	F9	CD
CC	9A	CE	CE	34	5C	46	16	B9	2E	F1	41	97	45	E7	B9
14	A8	62	5F	0F	F4	52	B3	09	36	57	70	F2	99	F8	62
E6	CF	05	14	70	06	5D	B7	0C	C2	41	9D	C6	F1	E6	A1
5C	4B	EB	16	E3	94	2C	22	A9	86	70	9D	AF	49	90	0D
4B	22	70	DF	FA	03	B5	C5	C6	A6	D0	8A	DE	DC	C2	6D
CE	C8	7E	29	35	8D	AC	43	13	91	84	E3	01	14	24	07
30	9A	C8	33	01	C7	39	08	34	AA	2F	9C	F2	45	B6	95

State Array 2.0

14	CB	86	34	D5	58	9B	9E	40	04	1A	2E	CE	AB	5B	5D
B5	66	F8	A4	8B	EC	CE	38	AA	3D	F0	C8	90	DD	3D	DD
5B	09	6E	35	B2	60	AC	CB	29	5B	8E	29	A3	18	F0	89
B0	E0	58	05	43	CB	69	83	46	40	A2	BD	DB	EB	74	91
F7	62	DD	87	3B	4F	BC	16	0E	99	D8	1B	48	70	73	DB
03	DA	5E	A3	8E	85	42	A9	BE	F0	AC	87	4E	70	1A	2F
A7	87	43	0E	BD	A1	0B	55	DB	D6	6B	16	9F	F6	69	1D
C3	F4	7A	43	D2	9C	00	99	A4	73	A4	61	F5	8E	47	E2
B2	28	3E	7D	03	E1	6F	DC	B2	B1	11	8C	D9	CE	7A	0A
03	14	B9	00	15	10	91	90	F9	D8	8E	59	E3	65	29	75
D3	F5	DC	86	58	FE	54	9E	E0	DB	17	D4	8C	D8	31	89
44	D4	AB	D9	DD	4F	D7	43	42	C4	A4	0B	29	43	CD	61
EE	A8	5C	A6	06	04	CE	98	0F	1F	78	76	79	5F	7C	D6
95	63	6E	D5	7C	43	4B	2A	70	E9	20	ED	28	F1	44	B6
AF	93	DE	E3	AC	BA	28	77	50	EB	0E	B9	F0	05	0C	6B
61	37	A8	A1	39	F2	FF	DB	57	35	69	B6	E9	7C	C6	EF

Mix Column Matrix M mod $m_2(x)$

03	02	01	01	01	01	01	01	01	01	01	01	01	01	01	01
02	03	02	01	01	01	01	01	01	01	01	01	01	01	01	01
01	02	03	02	01	01	01	01	01	01	01	01	01	01	01	01
01	01	02	03	02	01	01	01	01	01	01	01	01	01	01	01
01	01	01	02	03	02	01	01	01	01	01	01	01	01	01	01
01	01	01	01	02	03	02	01	01	01	01	01	01	01	01	01
01	01	01	01	01	02	03	02	01	01	01	01	01	01	01	01
01	01	01	01	01	01	02	03	02	01	01	01	01	01	01	01
01	01	01	01	01	01	01	02	03	02	01	01	01	01	01	01
01	01	01	01	01	01	01	01	02	03	02	01	01	01	01	01
01	01	01	01	01	01	01	01	01	02	03	02	01	01	01	01
01	01	01	01	01	01	01	01	01	01	02	03	02	01	01	01
01	01	01	01	01	01	01	01	01	01	01	02	03	02	01	01
01	01	01	01	01	01	01	01	01	01	01	01	02	03	02	01
01	01	01	01	01	01	01	01	01	01	01	01	01	02	03	02
01	01	01	01	01	01	01	01	01	01	01	01	01	01	02	03

State Array 2.1

E1	9E	42	01	3E	7C	2E	39	FA	FF	15	5C	B1	2B	09	62
AD	28	8E	CE	E9	68	D0	9D	6B	2B	32	C1	55	75	20	26
F0	3A	25	0C	35	0E	FB	49	E2	81	DB	CA	59	70	9C	79
DD	DF	7C	59	4B	1F	A8	73	3E	29	8F	74	16	2B	CA	6B
72	77	A9	3E	77	EB	10	40	90	52	93	7F	ED	08	AC	94
BF	66	07	07	9F	9F	48	DA	D8	DE	E3	41	27	2F	E2	AB
47	DE	AC	B9	C8	91	9A	E8	1C	99	A0	5E	6E	F4	CD	D2
AF	E4	35	C9	6F	00	E6	BB	77	FF	F7	34	E2	11	43	42
6D	D2	20	E5	19	F1	78	EE	07	2F	32	08	4A	BB	BE	12
EC	ED	12	88	CE	A6	7A	AB	80	E1	27	5D	FB	EA	77	D0
79	57	97	BD	BE	E5	28	5B	D6	7D	3E	06	DB	9F	E9	91
86	ED	90	57	0E	68	4A	9E	31	74	C8	A8	8F	4A	EA	C3
E6	74	EE	DD	B9	BB	72	C6	93	F9	4D	9E	6C	2D	C4	35
FF	76	43	E0	50	BC	A9	28	DA	7E	B4	8C	09	49	E0	4B
0B	78	B0	DF	C1	00	99	B0	12	02	A9	C7	3E	D8	39	DD
25	79	74	BD	D0	8D	93	62	85	B8	AE	A0	5F	ED	3F	DC

Inverse P-box Matrix P_1^{-1} mod $m_2(x)$

46	76	22	83	56	BD	FC	2A	1F	CD	81	84	3A	89	D8	28
A6	2C	65	34	45	A3	82	DF	3C	5A	0A	D0	04	AB	A8	F4
5E	78	FB	08	CA	6F	5B	8F	67	3E	31	74	44	94	A7	AE
75	BB	E0	0D	9F	F3	00	24	F2	CE	A5	88	A9	96	B6	69
EB	13	06	8A	14	1B	0F	9E	2E	8C	A0	AC	5D	99	EF	A1
F1	EA	7D	61	15	80	33	93	C6	BC	23	CB	62	DB	11	6A
FA	B3	66	6B	7A	D3	86	C4	0C	0E	1E	7B	F7	5C	05	BA
FE	97	7F	20	C0	C7	90	E5	CC	64	53	B2	DD	18	9D	B1
C9	ED	D4	E2	42	8B	AD	5F	07	85	1D	49	92	26	6C	36
3B	D9	3D	B5	EE	71	43	D1	F6	37	2B	21	9A	39	7E	F9
2D	B4	C1	09	68	BF	E1	E7	32	C5	02	4D	59	87	54	3F
16	C3	60	73	1A	F5	48	38	E4	7C	8D	77	10	AA	41	8E
E3	58	9C	19	FF	52	B7	01	4A	EC	17	25	57	B0	50	A4
A2	29	2F	B9	4F	AF	D2	CF	98	F0	DA	DE	E8	DC	03	4E
C2	6E	79	72	35	27	FD	E9	4B	55	63	4C	9B	47	BE	6D
40	F8	95	0B	E6	C8	70	30	D6	D5	D7	51	12	1C	91	B8

State Array 2.2

B9	E2	3E	D8	74	99	35	07	7C	8F	57	6B	78	59	7A	C8
9E	00	35	E9	77	EB	5C	DB	28	16	7F	9F	4B	D6	28	6D
73	74	F0	E5	C9	8F	DA	E2	25	75	AF	7D	28	15	19	70
42	97	32	91	DF	AC	85	E1	34	7E	E6	FF	D2	81	12	AE
62	C7	90	99	EE	77	E1	E0	5E	31	4A	BE	EA	C8	ED	08
3E	C3	27	5B	A9	77	72	6C	55	4D	ED	AC	A9	B9	42	77
CA	1F	BB	E9	AB	3A	FB	20	93	BD	8D	A8	12	3F	20	07
D2	DE	CA	74	90	01	AD	A8	8E	9C	10	4A	5D	0E	02	49
9F	79	DE	DD	86	80	9A	B4	57	FF	4B	D8	CE	06	A0	35
E8	DD	93	00	43	79	E0	9D	BB	50	F9	C4	59	B0	6F	3E
BE	D0	2B	66	5F	BD	9E	B0	78	DD	8C	76	0E	1C	74	2F
09	62	9E	D0	32	29	DF	6E	DC	2B	93	CE	A6	BF	39	E3
40	DB	09	C1	E6	27	F1	DA	AB	FA	A9	68	EE	EC	88	11
ED	FF	F4	48	E2	D0	12	91	0B	2B	9F	BC	49	C6	4A	E4
0C	A0	3E	B1	08	BB	94	F7	2D	43	68	3E	FB	6B	52	C1
EA	7C	E5	07	79	41	2F	72	26	B8	2E	25	47	CD	39	ED

Inverse Mix Column Matrix M^{-1} mod $m_1(x)$

2B	B0	76	69	5C	65	7E	55	7C	80	01	03	67	C4	62	05
B0	23	97	3A	A1	07	58	94	43	15	A6	CB	D7	4B	BF	62
76	97	5F	31	B2	C7	FB	A6	15	73	84	A1	89	9C	4B	C4
69	3A	31	89	B4	25	1F	A2	4E	A2	1F	25	B4	89	D7	67
5C	A1	B2	B4	A3	59	04	71	93	5A	36	B7	25	A1	CB	03
65	07	C7	25	59	0A	F2	0E	5E	C2	7A	36	1F	84	A6	01
7E	58	FB	1F	04	F2	4D	6E	EC	33	C2	5A	A2	73	15	80
55	94	A6	A2	71	0E	6E	51	FD	EC	5E	93	4E	15	43	7C
7C	43	15	4E	93	5E	EC	FD	51	6E	0E	71	A2	A6	94	55
80	15	73	A2	5A	C2	33	EC	6E	4D	F2	04	1F	FB	58	7E
01	A6	84	1F	36	7A	C2	5E	0E	F2	0A	59	25	C7	07	65
03	CB	A1	25	B7	36	5A	93	71	04	59	A3	B4	B2	A1	5C
67	D7	89	B4	25	1F	A2	4E	A2	1F	25	B4	89	31	3A	69
C4	4B	9C	89	A1	84	73	15	A6	FB	C7	B2	31	5F	97	76
62	BF	4B	D7	CB	A6	15	43	94	58	07	A1	3A	97	23	B0
05	62	C4	67	03	01	80	7C	55	7E	65	5C	69	76	B0	2B

State Array 2.3

60	74	3F	43	94	08	C5	4B	5A	AA	9C	2A	1E	56	0B	BC
12	87	2B	E4	AC	CA	DB	6F	E1	89	35	7A	09	AA	BB	79
33	0F	EC	72	F0	89	2D	B1	BC	8F	7F	85	1C	C8	5E	20
24	20	D8	35	CA	15	0C	16	6A	89	EA	21	D5	D0	47	80
E9	C3	79	F5	51	46	F1	EA	45	6B	98	81	18	37	B5	53
68	87	ED	D3	96	F1	5A	03	66	0D	35	DA	4F	4B	BC	EA
6F	F9	20	69	53	78	FD	35	72	66	EC	FF	D9	32	25	C2
B8	44	AF	14	F5	E3	EB	25	0B	FB	16	9E	03	62	05	82
2D	4A	5E	6A	04	91	83	92	A3	80	F1	42	3C	8D	5B	09
27	9E	9A	24	0E	29	C8	B5	5D	6E	61	C5	BD	6F	71	76
93	8D	31	65	B0	DC	1D	C6	05	C4	08	0E	E8	B7	BF	AE
73	40	B6	77	83	67	03	41	33	9D	1C	8C	DB	A1	F1	4E
F3	52	6D	A1	DD	D5	FD	82	CA	0B	81	D3	2D	E5	70	8B
D4	0D	EC	C1	2F	51	B4	EB	7F	F9	8C	59	82	BA	AF	5A
EC	69	7B	C9	D1	AF	65	5F	D9	65	EC	5F	3A	6B	FA	52
5D	A2	BF	17	D1	A6	29	CC	53	BE	15	AF	2B	28	4B	90

Inverse S-box Matrix S_1^{-1} mod $m_1(x)$

BB	1E	3E	23	5D	1D	BA	82	AB	FB	0F	6A	9F	BF	84	6F
DA	EA	73	BE	42	E2	E7	2B	CD	0D	E8	E9	13	62	35	59
21	B1	CC	26	E6	B0	E5	F0	88	7D	75	15	7C	7A	5F	77
9C	48	D2	4D	8F	7B	00	07	24	3B	93	F8	B3	0A	E1	38
CA	B4	58	F5	A2	67	78	68	85	CF	C0	C7	66	37	92	2D
9B	89	3D	5E	41	19	AE	50	44	94	C8	BD	AF	FD	1F	C5
31	29	A8	0B	B9	7E	96	E4	4E	61	F3	D5	69	20	74	79
71	18	05	98	80	2E	1C	5B	12	06	6D	8C	DC	25	AC	F1
51	D4	A1	DE	3C	39	3A	32	A5	F9	5A	B2	FF	43	EF	CE
33	2A	C9	EE	49	30	4B	5C	81	DB	F2	70	90	52	F6	FC
B5	1A	6E	C4	57	C1	56	D0	03	DD	D1	55	46	BC	2F	A0
C2	76	40	14	9A	16	0E	E3	0C	FA	4A	F4	4C	1B	CB	B6
8E	4F	3F	B7	83	7F	72	01	8D	E0	D7	D3	54	9E	60	FE
A6	AA	10	6B	34	95	A9	C6	27	C3	65	47	EC	11	2C	8A
EB	9D	17	A4	F7	45	B8	02	AD	D9	22	86	97	D6	64	A7
99	DF	87	36	28	63	ED	04	09	91	D8	53	A3	6C	8B	08

State Array 2.4

BA	68	36	8F	CF	51	AF	9A	C1	D1	E0	6E	9D	7E	C2	D3
B1	12	40	92	D7	46	1B	ED	35	81	5E	D0	33	D1	F4	5C
4D	99	60	F0	6F	81	10	E9	D3	09	04	44	4F	FF	45	3E
58	3E	43	5E	46	89	8E	29	56	81	2F	73	FD	BF	80	AB
F6	B3	5C	C5	E2	B9	59	2F	41	0E	F9	CD	D4	98	BD	7B
3A	12	2C	0A	61	59	C1	9C	96	A6	5E	BC	28	9A	D3	2F
ED	FC	3E	4B	7B	32	8A	5E	F0	96	60	08	52	26	3D	7C
B2	A2	D8	B4	C5	E1	CB	3D	C2	B6	29	D9	9C	E5	9B	88
10	57	45	56	CA	0D	24	7D	93	AB	59	E6	B7	27	16	33
05	D9	DD	58	EB	C9	FF	BD	95	B8	E7	AF	47	ED	2B	E4
3B	27	BE	AE	6A	9E	AA	69	9B	66	51	EB	EF	8C	53	22
07	5D	D5	5B	24	1C	9C	42	4D	C3	4F	8D	1B	E8	59	F7
38	B0	A9	E8	11	FD	8A	88	46	C2	CD	0A	10	1F	82	0C
37	A6	60	13	87	E2	C7	CB	04	FC	8D	30	88	55	D8	C1
60	4B	E3	90	62	D8	AE	63	52	AE	60	63	C4	0E	A0	B0
95	75	53	18	62	F3	C9	54	7B	86	89	D8	40	A1	9A	FB

Round Key 0

BA	78	16	BF	8F	01	CF	EA	41	41	40	DE	5D	AE	22	23
B0	03	61	A3	96	17	7A	9C	B4	10	FF	61	F2	00	15	AD
4F	8B	42	C2	2D	D3	72	9B	51	9B	A6	F6	8D	2D	A7	CC
5B	2D	60	6D	05	DA	ED	5A	D5	12	8C	C0	3E	6C	63	58
F2	A7	78	F1	A6	ED	3D	5B	C5	9A	5D	79	10	4C	59	8F
3F	07	09	3F	24	0C	A4	E9	13	33	FB	09	ED	4F	36	DA
EB	EA	18	7D	3D	64	EC	28	76	00	C6	BE	94	F0	DB	8A
B5	B5	FF	83	82	B6	AC	4A	45	21	8E	6E	5B	32	7C	7F
18	4F	6D	6E	82	55	4C	05	1B	33	F1	5E	7F	FF	FE	CB
0C	C0	F4	61	A2	90	96	C4	1C	21	4E	16	8E	34	C2	1D
31	3D	94	94	20	C4	C0	13	11	FC	FB	51	25	56	B9	D8
0C	46	FE	60	6F	47	F7	39	C6	58	E4	36	D0	33	B2	0C
34	AC	85	D4	5D	A1	E6	F4	CA	5E	61	B6	DC	C3	6E	F0
3A	BB	4D	2E	CA	BF	AA	B6	89	61	20	8D	45	88	35	3C
6E	55	CD	AE	2C	86	C0	1D	DC	30	CE	DD	0A	D0	4E	4E
9A	6A	7C	27	2D	AC	A6	2B	F4	19	26	67	8F	7E	75	04

State Array 3.0: Re-plaintext

00	10	20	30	40	50	60	70	80	90	A0	B0	C0	D0	E0	F0
01	11	21	31	41	51	61	71	81	91	A1	B1	C1	D1	E1	F1
02	12	22	32	42	52	62	72	82	92	A2	B2	C2	D2	E2	F2
03	13	23	33	43	53	63	73	83	93	A3	B3	C3	D3	E3	F3
04	14	24	34	44	54	64	74	84	94	A4	B4	C4	D4	E4	F4
05	15	25	35	45	55	65	75	85	95	A5	B5	C5	D5	E5	F5
06	16	26	36	46	56	66	76	86	96	A6	B6	C6	D6	E6	F6
07	17	27	37	47	57	67	77	87	97	A7	B7	C7	D7	E7	F7
08	18	28	38	48	58	68	78	88	98	A8	B8	C8	D8	E8	F8
09	19	29	39	49	59	69	79	89	99	A9	B9	C9	D9	E9	F9
0A	1A	2A	3A	4A	5A	6A	7A	8A	9A	AA	BA	CA	DA	EA	FA
0B	1B	2B	3B	4B	5B	6B	7B	8B	9B	AB	BB	CB	DB	EB	FB
0C	1C	2C	3C	4C	5C	6C	7C	8C	9C	AC	BC	CC	DC	EC	FC
0D	1D	2D	3D	4D	5D	6D	7D	8D	9D	AD	BD	CD	DD	ED	FD
0E	1E	2E	3E	4E	5E	6E	7E	8E	9E	AE	BE	CE	DE	EE	FE
0F	1F	2F	3F	4F	5F	6F	7F	8F	9F	AF	BF	CF	DF	EF	FF