The Ciência & Engenharia - Science & Engineering Journal
ISSN: 0103-944X
Volume 11 Issue 1, 2023
pp: 1825-1840

Incorporating a New Pseudorandom Number Generator in AES Algorithm to Improve Its Security Level

Dilshad Akhtar[1], M. R. Hassan[2], Neda Fatma[3]
1. Research Scholar, T.M. Bhagalpur University, Bhagalpur-812007 (India).
2. Professor, University Department of Mathematics, T. M. Bhagalpur University, Bhagalpur-812007 (India).
3. Research Scholar, T.M.Bhagalpur University, Bhagalpur-812007 (India).

Abstract:
The implementation of the multiplicative inverses of elemental polynomials under an irreducible polynomial over GF(p^n) played an important role in cryptography. In the AES algorithm, the multiplicative inverses under the first irreducible polynomial over GF(2^8) have been used for the first time in 1999 to design its substitution box. The new PRNG RC4-MI in which the multiplicative inverses under the two irreducible polynomials over GF(7^3) are being used accepts the AES key as its own key and generates random bytes. Undertaking exclusive OR operation of RC4-MI bytes with AES cipher bytes, one gets a new sequence of cipher bytes thatexhibits randomness quantitatively better than that of the original sequence of AES cipher bytes.

Keywords: AES algorithm, Irreducible polynomial, Multiplicative inverse, RC4-MI algorithm, Randomness.

1. Introduction:

The AES (Advanced Encryption Standard) is a symmetric block cipher selected by the U.S. government to protect secret information. AES is implemented in software and hardware throughout the world to encrypt sensitive information. It is important for government computer security, cybersecurity, and electronic data protection. AES has become the most important algorithm used in symmetric key cryptography. The transparent selection process established by NIST helped create a high level of confidence in AES among security and cryptography experts

In 1997, NIST started looking for a replacement for DES, which would be called the Advanced Encryption Standard or AES. The NIST specifications required a block size of 128 bits and three different key sizes of 128, 192, and 256 bits. The specifications also required that AES be an open algorithm, available to the public worldwide. The announcement was made internationally to solicit responses from all over the world.

After the First AES Candidate Conference, NIST announced that 15 out of 21 received algorithms had met the requirements and been selected as the first candidates (August 1998). Algorithms were submitted from a number of countries; the variety of these proposals demonstrated the openness of the process and worldwide participation.

After the Second AES Candidate Conference, which was held in Rome, NIST announced that 5 out of 15 candidates-MARS, RC6, Rijndael, Serpent, and Twofish-were selected as the finalists

The Ciência & Engenharia - Science & Engineering Journal
ISSN: 0103-944X
Volume 11 Issue 1, 2023
pp: 1825-1840

(August 1999). After the Third AES Candidate Conference, NIST announced that Rijndael, (pronounced like "Rain Doll"), designed by Belgian researchers Joan Daemen and Vincent Rijment, was selected as Advanced Encryption Standard (October 2000).

In February 2001, NIST announced that a Federal Information Processing Standard (FIPS) draft was available for public review and comment.Finally, AES was published as FIPS 197 in the Federal Register in December 2001.

The criteria defined by NIST for selecting AES fall into three categories: security, cost, and implementation. In the end, Rijndael was judged the best at meeting the combination of these criteria.

The main emphasis was on security. Because NIST explicitly demanded a 128-bit key, thiscriterion focused on resistance to cryptanalysis attacks other than a brute-force attack.

The second criterion was cost, which covers the computational efficiency and storage requirement for different implementations such as hardware, software, or smart cards.

This criterion included the requirement that the algorithm must have flexibility (be implementable on any platform) and simplicity.

R.A. Anderson et al (1998) proposed a new block cipher, Serpent, as a candidate for the Advanced Encryption Standard. This algorithm uses a new structure that simultaneously allows a more rapid avalanche, a more efficient bit-slice implementation, and an easy analysis that enables us to demonstrate its security against all known types of attacks. Although designed primarily for efficient implementation on Intel Pentium/MMX platforms, it is also suited for implementation on smartcards and other 8-bit processors. In this note, they describe why. They also describe why many other candidates are not suitable.

Isa, Herman &Bahari et al (2011) discussed the current security and efficiency analysis of its alternatives. TheAES(Advanced Encryption Standard) has been in existence for the last 11 years. It was widely accepted as the de facto standard in many security-related applications such as SSL/TLS, Microsoft BitLocker Drive Encryption, Skype, and many others. Recently in 2011, the AES was claimed to be theoretically broken in the single-key attack model using a new method called biclique. Just two years before in 2009, the AES with 192- and 256-bit keys were found to be theoretically broken in the related-key attack model. This paper reviews existing attacks on the AES and evaluates the efficiency of recent block cipher proposals as alternatives to the AES. These block ciphers were proposed to patch the AES against the related-key type of attack.

Alalak, Saif & Zukarnain et al (2013) improved the randomness of AES using MKP. Randomness is a high-impact property of the ciphertext that evaluates the strength of a cryptography system. TheAES(Advanced Encryption Standard) is a symmetric block cipher algorithm that passed the randomness test. AES algorithm is widely used in computer communication systems for secure data transfer. In previous work, they proposed a Multiple-key Protocol (MKP) for the AES algorithm. In this paper, they tested the randomness of the MKP-AES algorithm by using the diehard statistical tests software. The randomness of AES is improved when MKP is used.

Abdullah, Ako. (2017) provided an overview of AES. The AES (Advanced Encryption Standard) algorithm is one of the most common and widely symmetric block cipher algorithms used worldwide. This algorithm has its own particular structure to encrypt and decrypt secret data and is applied in hardware and software all over the world. It is extremely difficult for hackers to get

The Ciência & Engenharia - Science & Engineering Journal
ISSN: 0103-944X
Volume 11 Issue 1, 2023
pp: 1825-1840

real data when encrypting by the AES algorithm. Till date is not any evidence to crake the AES algorithm. AES has the ability to deal with three different key sizes such as AES 128, 192, and 256-bit, and each of these ciphers has a 128-bit block size. This paper provides an overview of the AES algorithm and explains several crucial features of this algorithm in detail and demonstration some previous research that have done on it incomparison to others such as DES, 3DES, Blowfish, etc.

De Los Reyes et al (2019) modified AES Cipher Round and Key Schedule. In this paper, Advanced Encryption Standard was modified to address the low diffusion rate at the early rounds by adding additional primitive operations such as exclusive OR and modulo arithmetic in the cipher round. Furthermore, byte substitution and round constant addition were appended to the key schedule algorithm. The modified AES was tested against the standard AES by means of avalanche effect and frequency test to measure the diffusion and confusion characteristics respectively. The results of the avalanche effect evaluation show that there was an average increase in the diffusion of 61.98% in round 1, 14.79% in round 2, and 13.87% in round 3. Consequently, the results of the frequency test demonstrated an improvement in the randomness of the ciphertext since the average difference between the number of ones to zeros is reduced from 11.6 to6.4 along with better-computed p-values. The results clearly show that the modified AES has improved diffusion and confusion properties and the ciphertext can still be successfully decrypted and recover back the original plaintext.

Sousiand Ahmad-Loayet al(2020) discussed the AES ciphering algorithm, explained the encryption & decryption process & evaluated the algorithm in comparison to DES. The AES algorithm proved to be one the most secure algorithms which allowed it to replace the DES algorithm altogether.

2. Explanation of AES:

The AES algorithm (also referred to as the Rijndael algorithm) is a symmetrical block cipher algorithm that uses 128,192, or 256-bit keys to transform a block of the 128-bit message into 128 bits of ciphertext which is the main reason why it is strong, secure and exponentially stronger than the DES in which 56-bit keys are used.

A substitution-permutation or SP network, with several rounds, is used by the AES algorithm to generate the ciphertext. The length of the keyin AES used will determine the number ofrounds.

For example, in the encryption process, the 128-bit keys consist of 10 rounds, 12 rounds for the 192-bit keys, and 14 rounds for 256-bit keys. In each case, all the rounds are identical except for the last round in which we won't have the mix column step.

Instead of having one line of bytes or bits like most ciphers, AES arranges them in a4x4 array.

The Ciência & Engenharia - Science & Engineering Journal
ISSN: 0103-944X
Volume 11 Issue 1, 2023
pp: 1825-1840

Byte 00	Byte 04	Byte 08	Byte 12
Byte 01	Byte 05	Byte 09	Byte 13
Byte 02	Byte 06	Byte 10	Byte 14
Byte 03	Byte 07	Byte 11	Byte 15

2.1 General Structure:

AES is an iterative instead of a Feistel cipher. It is based on two common techniques to encrypt and decrypt data knowns as substitution and permutation networks (SPN). The SPN is a number of mathematical operations which are carried out in block cipher algorithms. AES has the capacity to deal with 128 bits (16 bytes) as a fixed plaintext block size. These 16 bytes are represented in a 4x4 matrix and AES operates on a matrix of bytes. In addition, another crucial feature of the AES is the number of rounds. The number of rounds relies on the length of the key. There are three different key sizes are used by the AES algorithm to encrypt and decrypt data such as (128, 192, or 256 bits). The key sizes decide on the number of rounds such as AES uses 10 rounds for 128-bit keys, 12 rounds for 192-bit keys, and 14 rounds for 256-bit keys.

The input state array is XORed with the first four words of the key schedule before any round-based

processing for encryption can start. During the decryption process, the same thing happens, except that we now XOR the ciphertext state array with the last four key schedule words.

Each round consists of different four steps for encryption: Substitute bytes, Shift rows, Mix columns, and Add a round key. Lastly, we XOR the four words from the key schedule with the output of the previous three steps. Each round consists of different four steps for decryption: Inverse shift rows, Inverse substitute bytes, Add round key and Inverse mix columns. Finally, we XOR the four words from the key schedule with the output of the previous two steps. The last step in encryption does not have the mix columns, and the last step in decryption does not have the inverse mix columns step.

The Ciência & Engenharia - Science & Engineering Journal
ISSN: 0103-944X
Volume 11 Issue 1, 2023
pp: 1825-1840

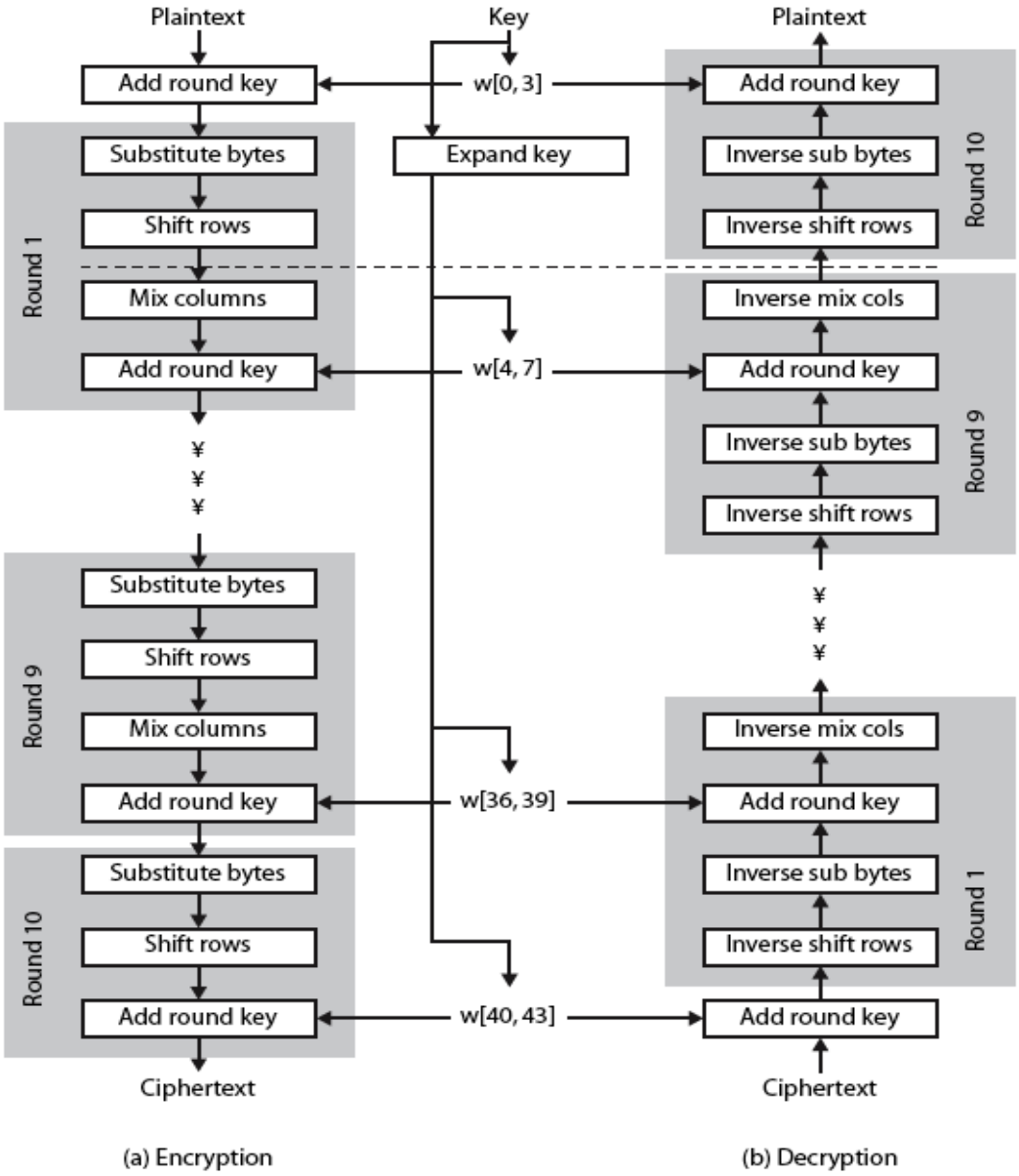

Figure-1: General Structure of AES Encryption. Algorithm.

2.2 Encryption Process:

As mentioned before, each round consists of a substitution step, a row-wise permutation step, a column-wise mixing step, and the addition of the round key. For encryption and decryption, the sequence in which these four steps are executed is different. While, overall, very similar steps are used in encryption and decryption, their execution is not equivalent and as previously stated, the order in which the steps are used

is different. The first step of the AES encryption algorithm is data substitution by using a substitution table. The second step is to exchange the data rows and the third step is to mix the columns. The last step is done using a different part of the encryption key expansion on each column. The first thing that happens under the AES encryption process is that your plaintext

The Ciência & Engenharia - Science & Engineering Journal
ISSN: 0103-944X
Volume 11 Issue 1, 2023
pp: 1825-1840

(which is the data you want to encrypt) is divided into blocks. The AES block size is 128 bits, so it divides the data into a 16-byte 4x4 column (16 x 8 = 128).
Then we will do a key expansion which involves taking the initial key and using it for each round of the encryption process to take with a set of other keys. With Rijndael's key schedule algorithm, these new 128-bit round keys are derived, which is basically an easy and fast way to generate new key ciphers.

I. Sub bytes (substitution of the bytes):
In the first step, we use a 16x16 lookup table to substitute the given bytes in theinput array. Using the notions of multiplicative inverses in GF(2^8) and bit scrambling, the entries in the lookup table are generated to remove the bit-level similarities inside each byte.

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

Table 1: AES S-box table.

The Ciência & Engenharia - Science & Engineering Journal
ISSN: 0103-944X
Volume 11 Issue 1, 2023
pp: 1825-1840

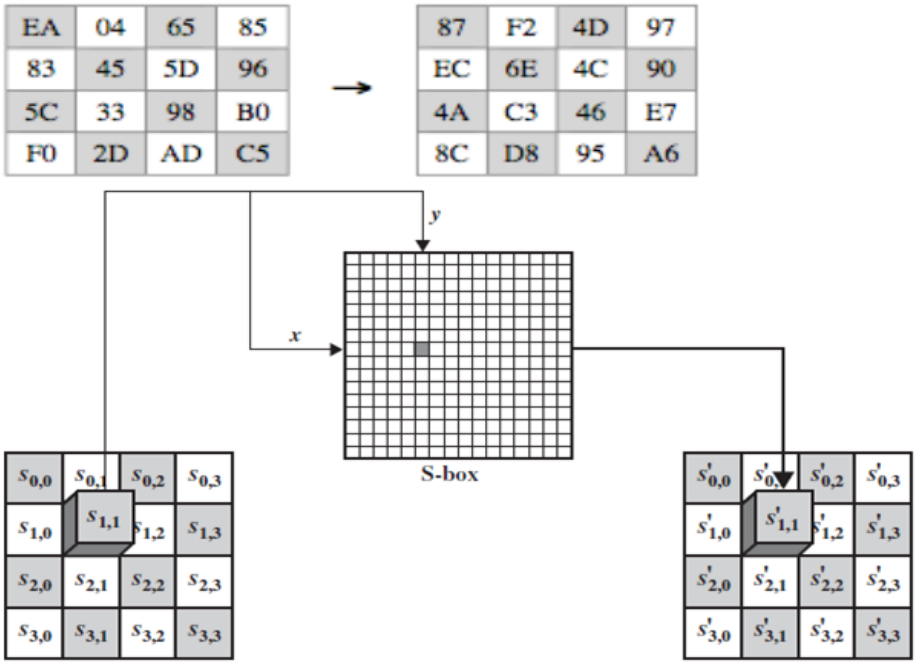

Figure-2: Substitution of the bytes.

II. Shift rows:

This step is the permutation step. All the rows except the first one are shifted, the second row will be shifted one space to the left, the third row should be shifted two spaces to the left and the fourth row should be shifted three spaces to the left as seen below:

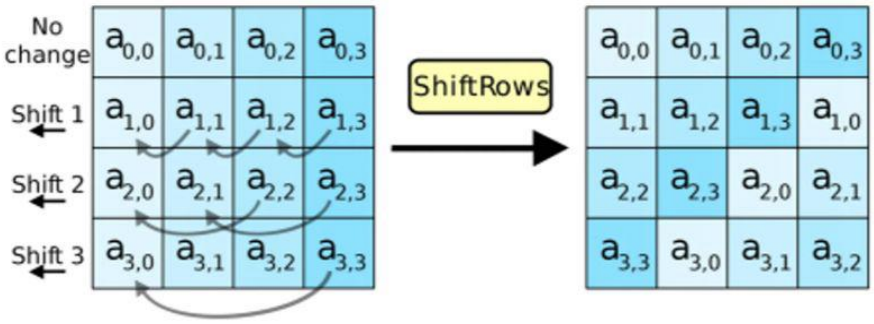

Figure-3: Shift rows.

After 10 rounds of processing, the shift-rows step along with the mix-column step makes every bit of the ciphertext to depend on every bit of the plaintext.

III. Mix columns:

In the third step, the Hill cipher is used by changing the block's columns to mix up the message more or we can say that in order to further diffuse it, every column has a mathematical equation applied to it.

The Ciência & Engenharia - Science & Engineering Journal
ISSN: 0103-944X
Volume 11 Issue 1, 2023
pp: 1825-1840

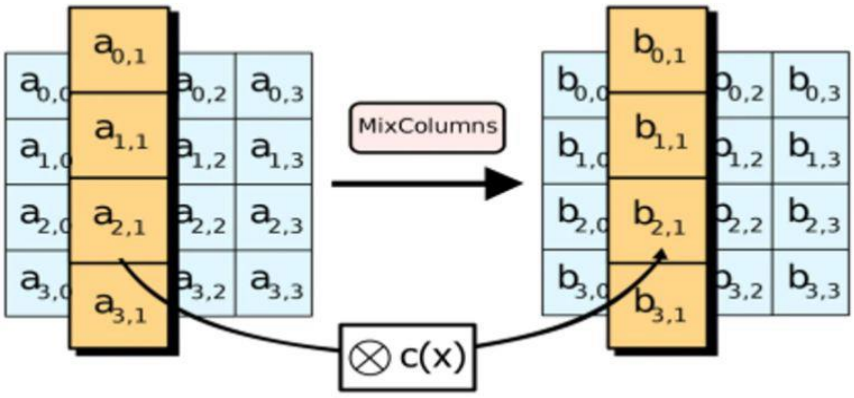

Figure-4: Mix columns.

IV. Add round keys:

In the final step, the result of the mixed columns is XORED with the first round key that was derived from the start using the initial key and Rijndael's key schedule.

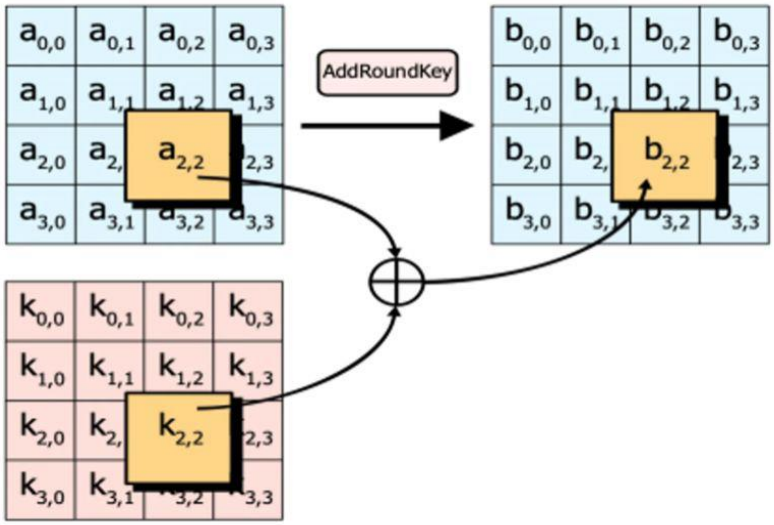

Figure-5: Add round keys.

2.3 Decryption Process:

Decryption is the process to obtain the original data that was encrypted. This process is based on the key that was received from the senderof the data. Both the senderand the receiver have the same key for the encryption & decryption of data. This process is similar tothe encryption process; however, in the reverse order.Decryption starts with an initial round, followed by 9 iterations of an "inverse normal round" andends with an "Add Round Key". An "inverse normal round" consists of the operations"Add Round Key", "Inv. Mix Columns", "Inv. Shift Rows" & "Inv. Sub Bytes" respectively. The last round consists of the same operations of an "inverse normal round" except for the"Inv. Mix Columns".

The Ciência & Engenharia - Science & Engineering Journal
ISSN: 0103-944X
Volume 11 Issue 1, 2023
pp: 1825-1840

I. Add round keys:

In the last round, we perform the Add Round Keys as performed in the encryption algorithm in the previous section. We perform the XOR operation between the cipher text and the expanded key corresponding to the particular iteration. Let's take the following figure with the diagrams on the left represent the cipher and the key values & the one on the right has the generated final value.

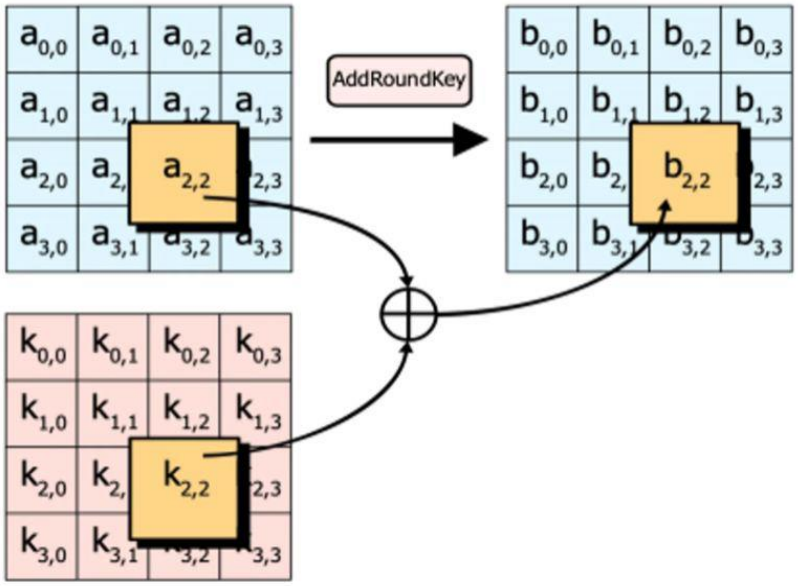

Figure-6: Add round keys.

II. Inverse shift rows:

In this step, we rotate each ith row by i elements to the right, as shown in the figure below:

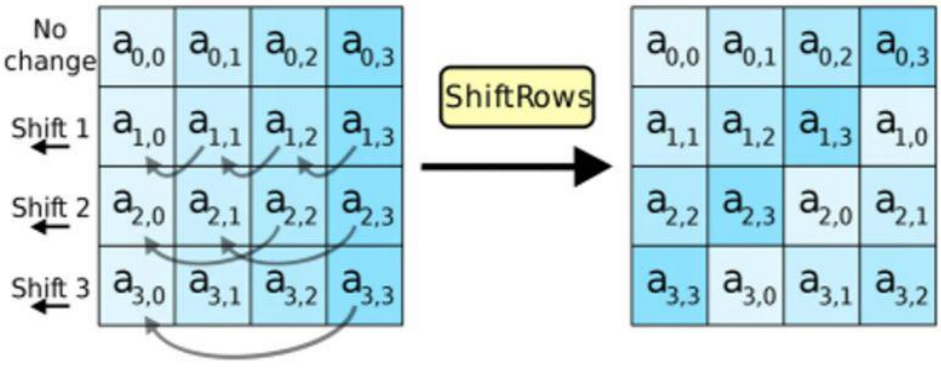

Figure-7: Inverse Shift Rows.

III. Inverse byte substitution:

In this step, we replace each entry in the matrix from the corresponding entry in the inverse S-Box, as shown in figure below.

The Ciência & Engenharia - Science & Engineering Journal
ISSN: 0103-944X
Volume 11 Issue 1, 2023
pp: 1825-1840

		y															
		0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
x	0	52	09	6a	d5	30	36	a5	38	bf	40	a3	9e	81	f3	d7	fb
	1	7c	e3	39	82	9b	2f	ff	87	34	8e	43	44	c4	de	e9	cb
	2	54	7b	94	32	a6	c2	23	3d	ee	4c	95	0b	42	fa	c3	4e
	3	08	2e	a1	66	28	d9	24	b2	76	5b	a2	49	6d	8b	d1	25
	4	72	f8	f6	64	86	68	98	16	d4	a4	5c	cc	5d	65	b6	92
	5	6c	70	48	50	fd	ed	b9	da	5e	15	46	57	a7	8d	9d	84
	6	90	d8	ab	00	8c	bc	d3	0a	f7	e4	58	05	b8	b3	45	06
	7	d0	2c	1e	8f	ca	3f	0f	02	c1	af	bd	03	01	13	8a	6b
	8	3a	91	11	41	4f	67	dc	ea	97	f2	cf	ce	f0	b4	e6	73
	9	96	ac	74	22	e7	ad	35	85	e2	f9	37	e8	1c	75	df	6e
	a	47	f1	1a	71	1d	29	c5	89	6f	b7	62	0e	aa	18	be	1b
	b	fc	56	3e	4b	c6	d2	79	20	9a	db	c0	fe	78	cd	5a	f4
	c	1f	dd	a8	33	88	07	c7	31	b1	12	10	59	27	80	ec	5f
	d	60	51	7f	a9	19	b5	4a	0d	2d	e5	7a	9f	93	c9	9c	ef
	e	a0	e0	3b	4d	ae	2a	f5	b0	c8	eb	bb	3c	83	53	99	61
	f	17	2b	04	7e	ba	77	d6	26	e1	69	14	63	55	21	0c	7d

Table-2: Inverse S-Box table.

We now perform the following operations 9 times (9 iterations):
IV. Add Round Key in iteration stage (same as previous step).

V. Inverse mix columns in iteration stage.
This operation is performed by the Rijndael cipher and it acts as the primary source of all the 10 rounds of diffusion in Rijndael. Each column is treated as a polynomial over Galois Field and multiplied by a fixed inverse polynomial as shown below.

$$\begin{bmatrix} r_0 \\ r_1 \\ r_2 \\ r_3 \end{bmatrix} = \begin{bmatrix} 14 & 11 & 13 & 9 \\ 9 & 14 & 11 & 13 \\ 13 & 9 & 14 & 11 \\ 11 & 13 & 9 & 14 \end{bmatrix} \begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \end{bmatrix}$$

VI. Inverse shift rows in the iteration stage (same as the previous step).
VII. Inverse byte substitution in the iteration stage (same as the previous step)

The Ciência & Engenharia - Science & Engineering Journal
ISSN: 0103-944X
Volume 11 Issue 1, 2023
pp: 1825-1840

2.4AES Key Expansion:

The AES algorithm is based on AES key expansion to encrypt and decrypt data. It is another most important step in the AES structure. Each round has a new key. In this section concentrates on the AES Key Expansion technique. The key expansion routine creates round keys word by word, where a word is an array of four bytes. The routine creates 4x (Nr+1) words. Where Nr is the number of rounds. The process is as follows:

The cipher key (initial key) is used to create the first four words. The size of the key consists of 16 bytes (k0 to k15) as shown in Fig.8 that represents in an array. The first four bytes (k0 to k3) represent as w0, the next four bytes (k4 to k7) in the first column represents as w1, and so on. We can use the particular equation to calculate and find keys in each round easily as follows:

• **K [n]: w[i] = k [n-1]: w[i] XOR k[n]: w[i].**

This equation uses to find a key for each round rather than w0. For w0 we have to use a particular equation that is different from the above equation.

• **K[n]: w0 = k [n-1]: w0 XOR SubByte (k [n-1]: w3>>8) XOR Rcon [i].**

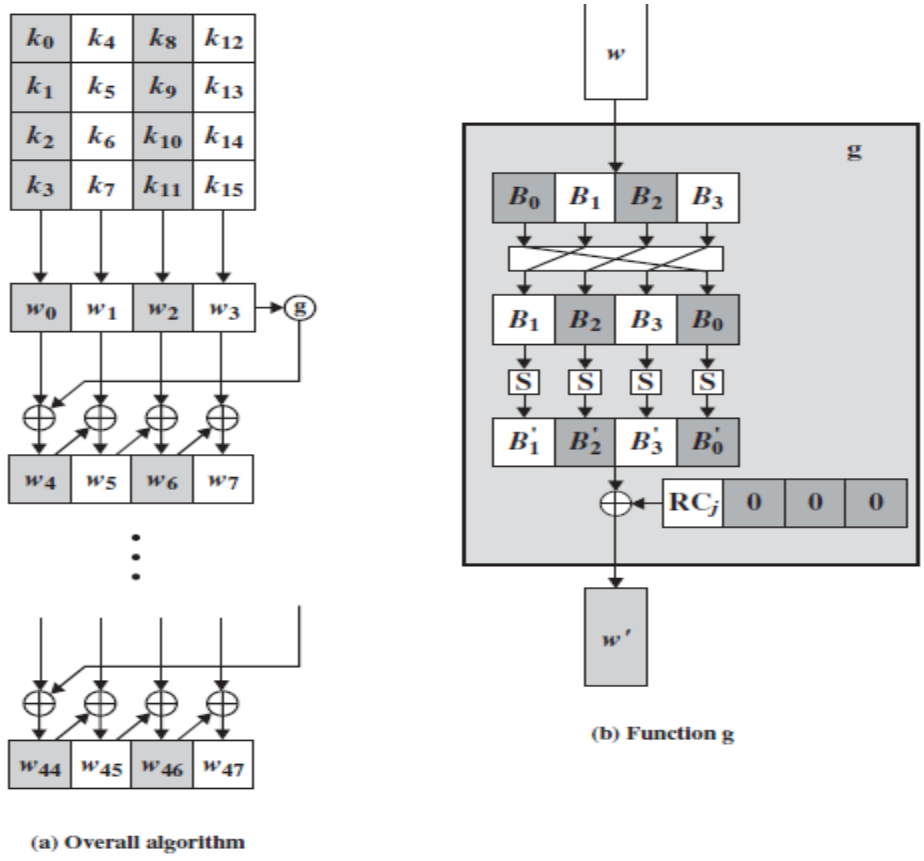

Figure-8: Key Expansion.

3. Pseudorandom Number Generator RC4-MI:

The proposed pseudorandom number generator (PRNG) known as RC4-MI is some modification of RC4 and NGG stream ciphers. The algorithm of RC4-MI is designed in two stages like in the original RC4 first is KSA and the other is PRGA. In this algorithm two S-boxes S1 and S2 are

The Ciência & Engenharia - Science & Engineering Journal
ISSN: 0103-944X
Volume 11 Issue 1, 2023
pp: 1825-1840

used. In the first S-box S1 and the key array K, the multiplicative inverses of elemental polynomials under the irreducible polynomial x^3+6x^2+4x+1 over $GF(7^3)$ are used and in the second S-box S2, the multiplicative inverses of elemental polynomials under the irreducible polynomial x^3+4x+1over $GF(7^3)$ are used. The elementary operations can be summarized as below.

```
Input: 1. Precomputed random array a[0, 1, …., 255].
       2. Precomputed random secret key array K.
Initialization:
       for i = 0, 1,…., 255
       j = 0 ;
       S1[i] = ai ;
       T[i] = K[i mod keylen] ;
Scrambling:
       for i = 0, 1, …, 255
       j = ( S1[ ( j + S1[i] + T[i] ) mod 256 ) mod 256 ;
       swap ( S1[i], S1[j] ) ;
```

Algorithm: RC4-MI KSA

```
Input: 1. Key-dependent scrambled array S1[0, 1, …, 255].
       2. Precomputed random array b[0, 1, …, 255].
Output: Pseudorandom keystream bytes Z.
Initialization:
       i = j = 0 ;
Output keystream generation loop:
       for i = 0, 1, …, 255 ;
       i = ( i + 1 ) mod 256 ;
       j = ( j + S1[i] ) mod 256 ;
       swap ( S1[i], S1[j] ) ;
       t = S2[ ( S1[i] + S1[j] ) mod 256]
       output Z = S[t] ;
```

Algorithm: RC4-MI PRGA

4. Incorporating a suitable PRNG RC4-MI:

Recently a newly designed PRNG(RC4-MI)discussed in section 3 is innovatively incorporated into the AES algorithm to present a new algorithm named Randomized AES (RAES). The output cipher text obtained by the proposed algorithm RAES is tested statistically and observed that the randomness is remarkably improved. A schematic diagram of the RAES encryption process is shown in Figure 9 in which the given 4-character key is shown being accepted by both AES as

The Ciência & Engenharia - Science & Engineering Journal
ISSN: 0103-944X
Volume 11 Issue 1, 2023
pp: 1825-1840

well as RC4-MI. An exclusive OR operation is undertaken between the 128 output bits and the 128 random bits of RC4-MI producing 128 cipher bits of RAES.

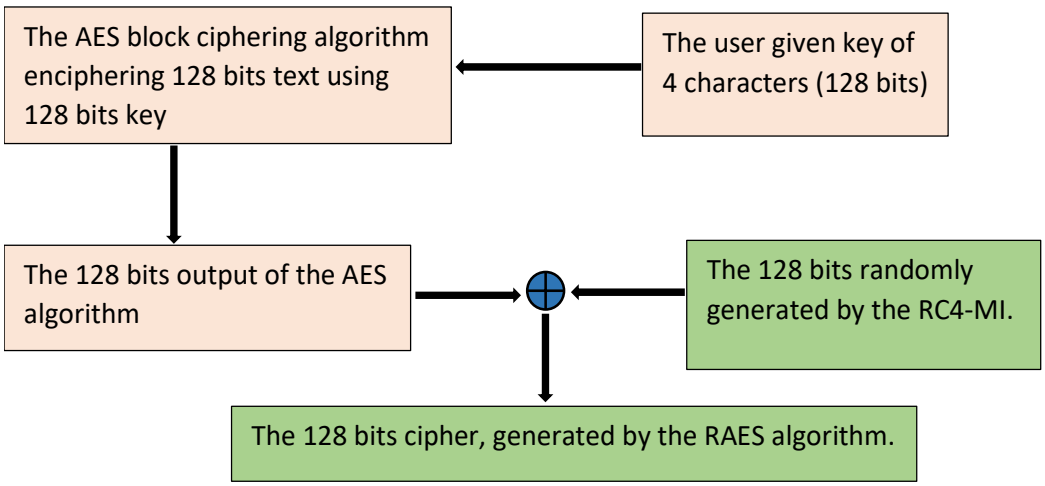

Figure-9: Schematic diagram of RAES encryption algorithm.

The PRNG RC4-MI is added to the AES encryption algorithm (Figure-10) after execution of the final round at the end of the 10^{th} round to design the RAES. The algorithmic flow of the RAES encryption is given in Figure 10 where it is shown that exclusive OR operation is executed between the 128 output bits of AES and the 128 random bits generated by RC4-MI at the lower right corner of the thick lined box. The same procedure continues for the next blocks till the end of the message. The algorithmic flow of the RAES decryption is given in Figure 11. From this figure, it is evident that exclusive OR operation is undertaken between the 128 random bits generated by RC4-MI and the 128cipher bits before starting the initial permutation shown at the upper right corner of the thick lined box.

The Ciência & Engenharia - Science & Engineering Journal
ISSN: 0103-944X
Volume 11 Issue 1, 2023
pp: 1825-1840

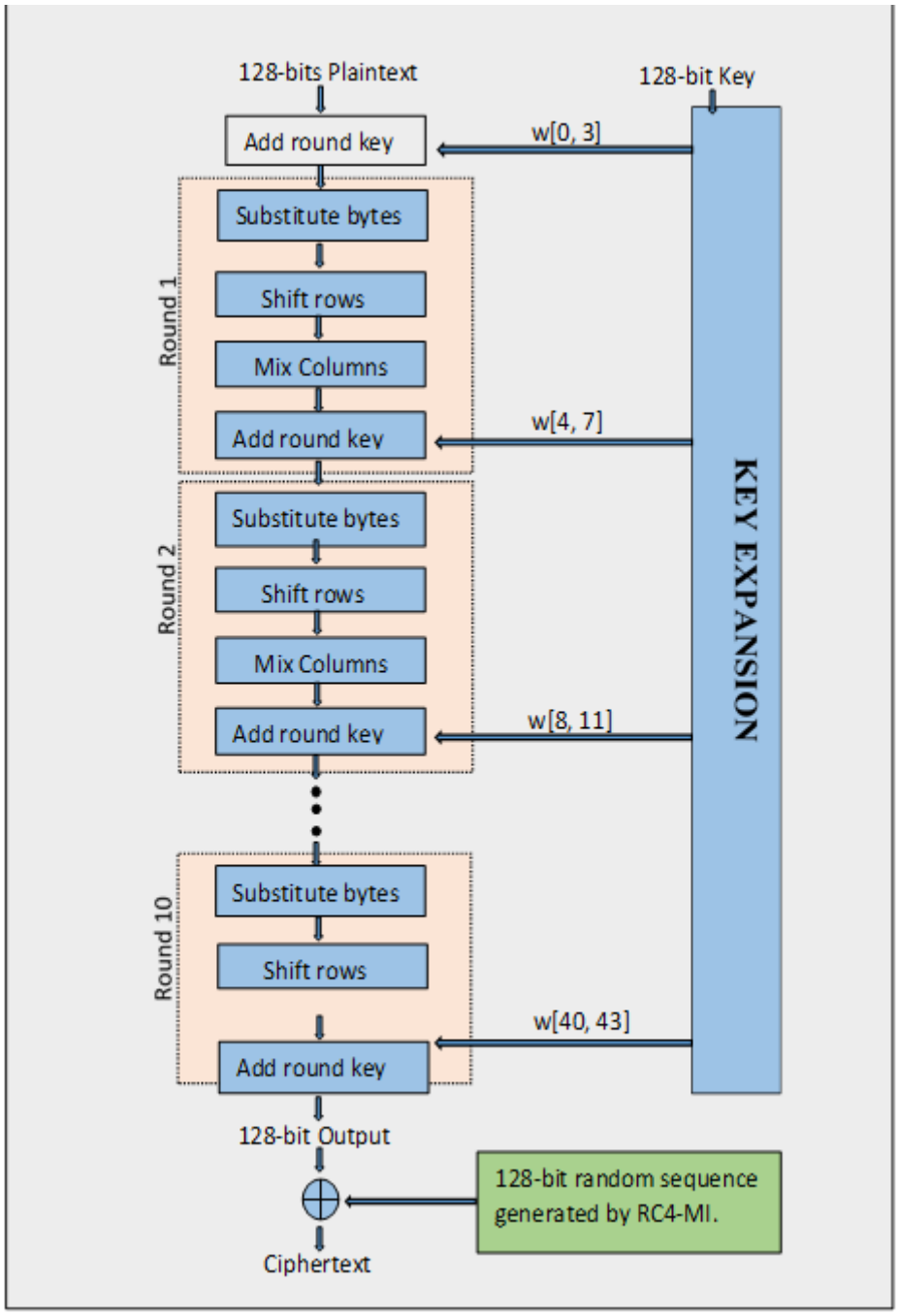

Figure-10: RAES Encryption method.

The Ciência & Engenharia - Science & Engineering Journal
ISSN: 0103-944X
Volume 11 Issue 1, 2023
pp: 1825-1840

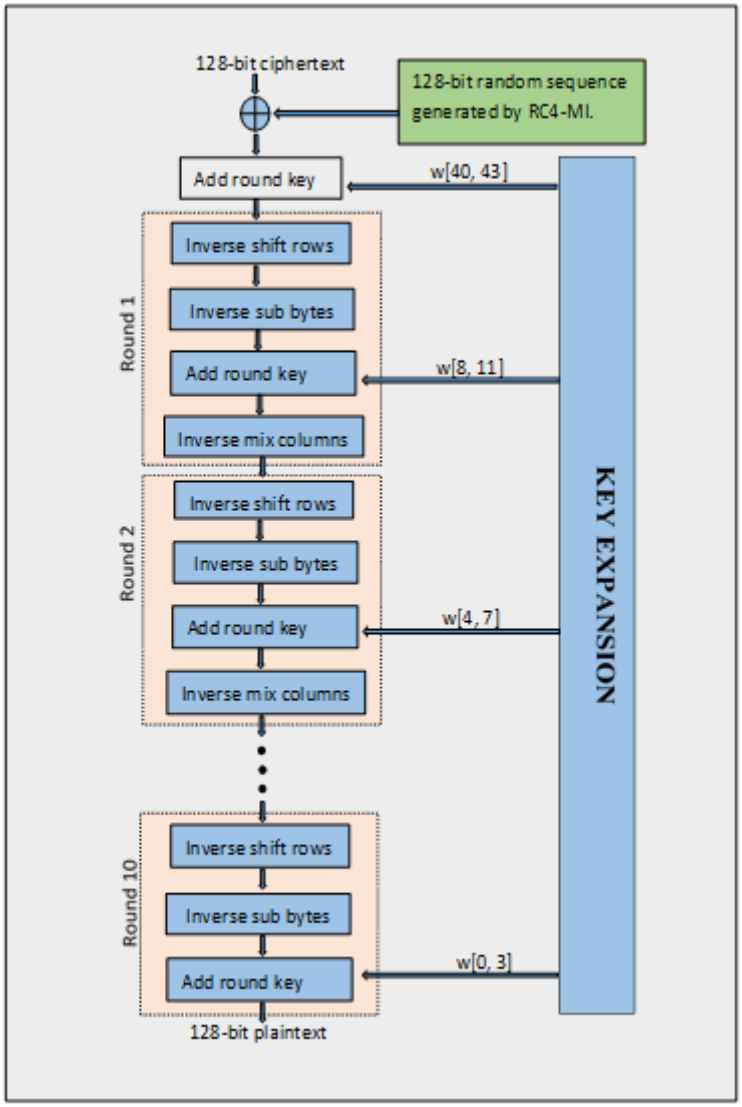

Figure-11: RAES Decryption method.

5. Conclusion:

In section 1, we have discussed the history of the AES algorithm and its related work. In section 2 the AES algorithm has been explained in detail in which the basic structure of it is shown in Figure 1. In section 2.5, we have explained the decryption process of the AES algorithm which is shown in Figure 6. In section 3, the AES algorithm has been modified by using a suitable PRNG RC4-MI which is named as RAES algorithm. The RAES algorithm produces a quantitatively better random cipher than the cipher produced by the AES algorithm. The RAES shows improvement in randomness due to the incorporation of RC4-MI because it produces a random byte in each execution.

6. Reference:

[1] R.A. Anderson, E. Biham, L.R. Knudsen, "Serpent", Proc. of the 1st AES candidate conference, CD-l: Documentation, August 20-22, 1998, Ventura.

[2] Yenuguvanilanka, J., &Elkeelany, O. (2008, April). Performance evaluation of hardware models of Advanced Encryption Standard (AES) algorithm. In Southeastcon, 2008. IEEE (pp. 222-225).

[3] Thangamayan, S., Kumar, B., Umamaheswari, K., Kumar, M. A., Dhabliya, D., Prabu, S., & Rajesh, N. (2022). Stock Price Prediction using Hybrid Deep Learning Technique for Accurate Performance. 2022 International Conference on Knowledge Engineering and Communication Systems (ICKES), 1–6. IEEE.

[4] Stallings, W., "Finite Fields," in Cryptography and Network Security Principles and Practices, 4th ed., Delhi, Pearson Education, 95-133(2008).

[5] Forouzan, B.A., Mukhopadhyay, D., "Mathematics of Cryptography," in Cryptography and Network Security, 2nd ed., New Delhi, TMH, 15-43 (2011).

[6] Knuth, D.E.: The Art of Computer Programming Seminumerical Algorithms, 3rd edn, vol. 2. Pearson Education, Upper Saddle River (2011).

[7] Singh, G. (2013). A study of encryption algorithms (RSA, DES, 3DES and AES) for information security. International Journal of Computer Applications, 67(19).

[8] Abdullah, A. M., & Aziz, R. H. H. (2016, June). New Approaches to Encrypt and Decrypt Data in Image using Cryptography and Steganography Algorithm., International Journal of Computer Applications, Vol. 143, No.4 (pp. 11-17).

[9] Joshi, K., Kumar, V., Sundaresan, V., Karanam, S. A. K., Dhabliya, D., Shadrach, F. D., & Ramachandra, A. C. (2022). Intelligent Fusion Approach for MRI and CT Imaging using CNN with Wavelet Transform Approach. 2022 International Conference on Knowledge Engineering and Communication Systems (ICKES), 1–6. IEEE.

[10] Abdullah, Ako. (2017), Advanced Encryption Standard (AES) Algorithm to Encrypt and Decrypt Data. https://www.researchgate.net/publication/317615794

[11] De Los Reyes, Edjie&Sison, Ariel & Medina, R.P.. (2019). Modified AES Cipher Round and Key Schedule. Indonesian Journal of Electrical Engineering and Informatics. 7. 28-35. 10.11591/ijeei.v7i1.652.

[12] Bhargav, S., Majumdar, A., &Ramudit, S. (2008, Spring). 128-bit AES decryption. Retrieved November 21, 2020, from http://www.cs.columbia.edu/~sedwards/classes/2008/4840/reports/AES.pdf

[13] Clark, A. (2018, August 2). How much encryption is too much: 128, 256 or 512-bit? Retrieved November 21, 2020, from https://discover.realvnc.com/blog/how-much-encryption-is-too-much-128-256-or-512-bit