The Ciência & Engenharia - Science & Engineering Journal
ISSN: 0103-944X
Volume 11 Issue 1, 2023
pp: 1841-1853

Incorporating the New PRNG in Advance Encryption Standard

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

Abstract
This manuscript explores the fusion of two well-known encryption algorithms, the Advanced Encryption Standard (AES) and the Rivest Cipher (RC4), resulting in a novel encryption algorithm called AES-RC4. AES-RC4 is a block cipher that combines the strengths of AES with a variant of RC4 called RC4-GF, developed by ourselves. RC4-GF incorporates additional steps compared to AES, resulting in a more intricate ciphertext generation process.
The introduction of AES-RC4 brings forth a highly secure encryption technique with increased complexity in the ciphertext compared to traditional AES. By leveraging the combined capabilities of AES and the modified RC4-GF, AES-RC4 offers enhanced encryption strength and improved resistance against cryptographic attacks.
Keywords AES, RC4, Variant of RC4, Block Cipher

1. introduction

Every individual requires privacy, especially when dealing with highly sensitive data. It is essential to be able to conceal this data from unauthorized individuals and only share it with trusted parties.Earlier, humans utilized basic techniques to conceal messages; however, these methods proved to be insufficient as threats to computer and network security continued to escalate. Consequently, researchers have consistently been driven to enhance encryption techniques. As part of this endeavour, the Data Encryption Standard (DES) was introduced by International Business Machines (IBM). DES was developed as a modification of the existing Lucifer algorithm and was subsequently adopted by the National Institute of Standards and Technology (NIST) in 1977. The goal was to establish a more robust encryption standard that could withstand evolving security challenges.
But DES became useless after 1990 as its short key is susceptible to Brute Force attacks performing 56 bits key exhaustive search attacks. It may also be noted that there are initiatives to undertake improvement on DES itself and in this order double DES was introduced. The Double DES uses two keys each of 56 bits and a text of 64 bits and a cipher obtained using the first key is again encrypted using the second key. After thattwo types of Triple DES were developed in 1998-99. Triple DES is still acceptable for federal use until 2030 but it is very slow for efficiency as DES because it has three times as many rounds as DES.
To address the challenges in encryption algorithms, the National Institute of Standards and Technology (NIST) initiated a competition in January 1997. This competition allowed individuals worldwide to participate in developing a successor to DES, which was named the Advanced

The Ciência & Engenharia - Science & Engineering Journal
ISSN: 0103-944X
Volume 11 Issue 1, 2023
pp: 1841-1853

Encryption Standard (AES). The primary objective was to create a new encryption algorithm capable of rapidly protecting sensitive information.

The competition had specific requirements for the winning algorithm. AES was required to have a block length of 128 bits and a key length of 128, 192, or 256 bits, depending on the number of rounds. On November 26, 2001, AES was adopted as a standard, and it was published as FIPS 197 in the Federal Register on December 4, 2001.

The AES algorithm chosen as the winner was Rijndael, which had been invented by two Belgian researchers, Joan Daemen and Vincent Rijmen. During the evaluation process, AES candidates were assessed based on three primary criteria: security, cost, and algorithm and implementation characteristics. These evaluations ensured that the selected algorithm met stringent standards for its effectiveness, efficiency, and practicality.

'Security' of the proposed algorithm was most essential, and if an algorithmwas found not to be secure would not be consideredfurther. 'Cost' refers to the computationalefficiency (speed and memory requirements) of various types of implementations,including software, hardware and smart cards. Algorithm and implementationcharacteristics include flexibility and algorithm simplicity, among otherfactors.In the end, the five finalists were all felt to be secure. But Rijndael was selectedbecause of its combination of security, performance, efficiency, implementation ability, andflexibility werefound superior in comparison to the other finalists.

Eli Biham et al (2001) [3] present attacks on 7^{th}, 8^{th} and 10^{th} round on variants of Serpent. Serpent is one of the 5 AES finalists. They attack a 7^{th} round variant with all key lengths and 8^{th}& 10^{th} round variants with 256-bit keys. The attack enhances the amplified boomerang attack and uses better differentials. They also present the best 3^{rd}, 4^{th}, 5^{th} and 6^{th} round differential characteristics of Serpent.

Esa et al (2011) [5] present a paper that reviews existing attacks of the AES and proposed an algorithm for block cipher as alternative to the AES. They claimed that the presented block cipher algorithm were proposed to patch the AES against the related-key type of attack.

Abdullah, Ako. (2017) [7] deals with AES algorithm and explain several crucial features of this algorithm in details. They provide comparison of AES to the other algorithms such as DES, 3DES, Blowfish etc.

2.Detailed Overviews Of The Des Algorithm

DES algorithm used 64-bit plaintext and 64-bit key to provide a 64-bit ciphertext. In the 64-bit key, every 8^{th} bit is used as a parity checking bit therefore 56 bits of key are used in the algorithm to encrypt data. Firstly, the "initial permutation" step is done on the 64-bit plaintext which provides 64-bit output. The 64-bit key is being started with"permutation choice1" (PC1). The output of PC1 is 56 bits by ignoring themultiples of 8 bits. The two outputs of PC1 are fed to the 1^{st} round in the sequence of sixteen round blocks. The round block divides its input into two equal parts, the data bits have parts LPT of32 bits and RPT of 32 bits. Similarly, key bits are divided into two parts LKB and RKB each have 28 bits in length. The 56 bits are used to generate the 48-bit round key through the "permutation chooice2" (PC2). The 32-bit RPT is expanded to a 48-bit round key through "expansion permutation". The output from the PC2 block is XORed with an expansion permutation block to get the 48-bit address for the substitution box (S-box). The 48-bit

The Ciência & Engenharia - Science & Engineering Journal
ISSN: 0103-944X
Volume 11 Issue 1, 2023
pp: 1841-1853

are given as a sequence to S-box into 8 sections each of 6-bit. The S-box replaces every 6-bit of data to 4-bit data. The 32-bit from S-box is sent to the "permutation function" to provide more diffusion of bits. "Permutation function" bits are XOR-ed with the 32-bit LPT. This output of XOR is connected to the RPT of the next round. The LPT of the next round is connected to the RPT of this round. The output from LPT of 32-bit and RPT 32-bit is feed to the "Final Permutation" (inverse of initial permutation). The output of 64-bit is obtained from the final Permutation. All the steps of the DES encryption algorithm are clearly represented in the Fig. 1.

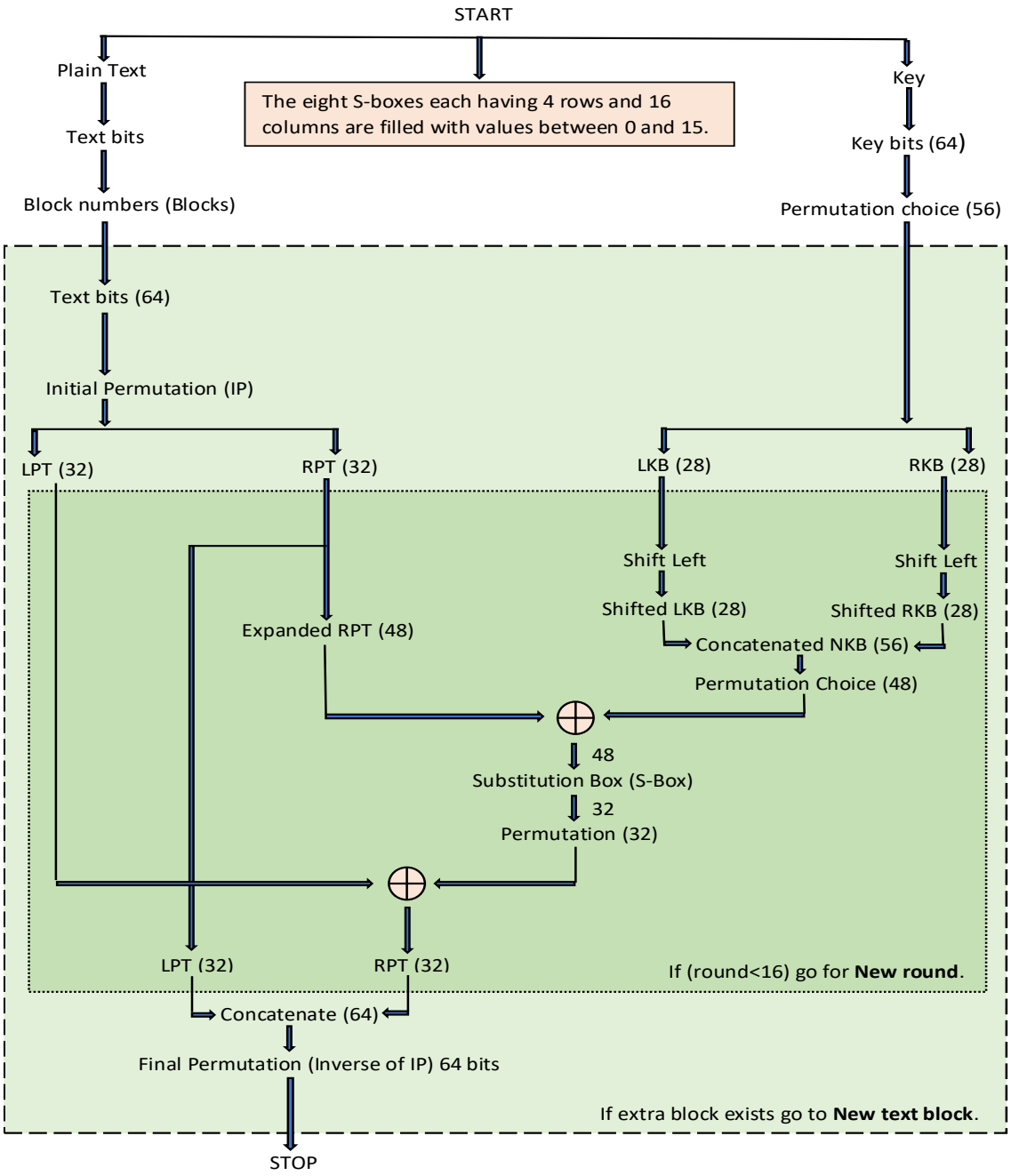


Fig.1 : Algorithmic flow of the DES Encryption

The Ciência & Engenharia - Science & Engineering Journal
ISSN: 0103-944X
Volume 11 Issue 1, 2023
pp: 1841-1853

3.1 Detailed Overviews Of AES Algorithm

The AES algorithm is a symmetrical block cipher algorithm that uses 128,192 or 256-bit keys to transform a block of 128-bit messages into a 128-bit of ciphertext.Because the key of AES has more bits than any previous encryption algorithm therefore AES is more stronger and secure from any cyber- attack than the previous encryption algorithmas the previous algorithm usesless than64-bit key. AES is a roundbased algorithm and the roundsdepend on the length of the key. In the encryption process the 128, 192 and 256-bit keys consist of 10, 12 and 14 rounds respectively.Before the rounds for encryption start,the input state array is XORed with the first 128bits of the key schedule. Each round except the last round consists of the following four steps for encryption:

Substitute bytes, Shift rows, Mixcolumns and Add round key. But the last round does not have the mix columns step.i.e. in the last round we XOR the four words (i.e. 128 bits) from the key schedule with theoutput of the previous two steps (Substitute bytes and Shift rows). During decryption,we now XOR the ciphertext state array with the last four key schedule words. Similarly,each round except the last consists of the following four steps for decryption:

Inverse shift rows, Inversesubstitute bytes, Add round key and Inverse mix columns and the last round does not have the inverse mix columns step. i.e,lastly we XOR the four words fromthe keyschedule with the output of the previous two steps. Figure of AES given in Fig. 2.1

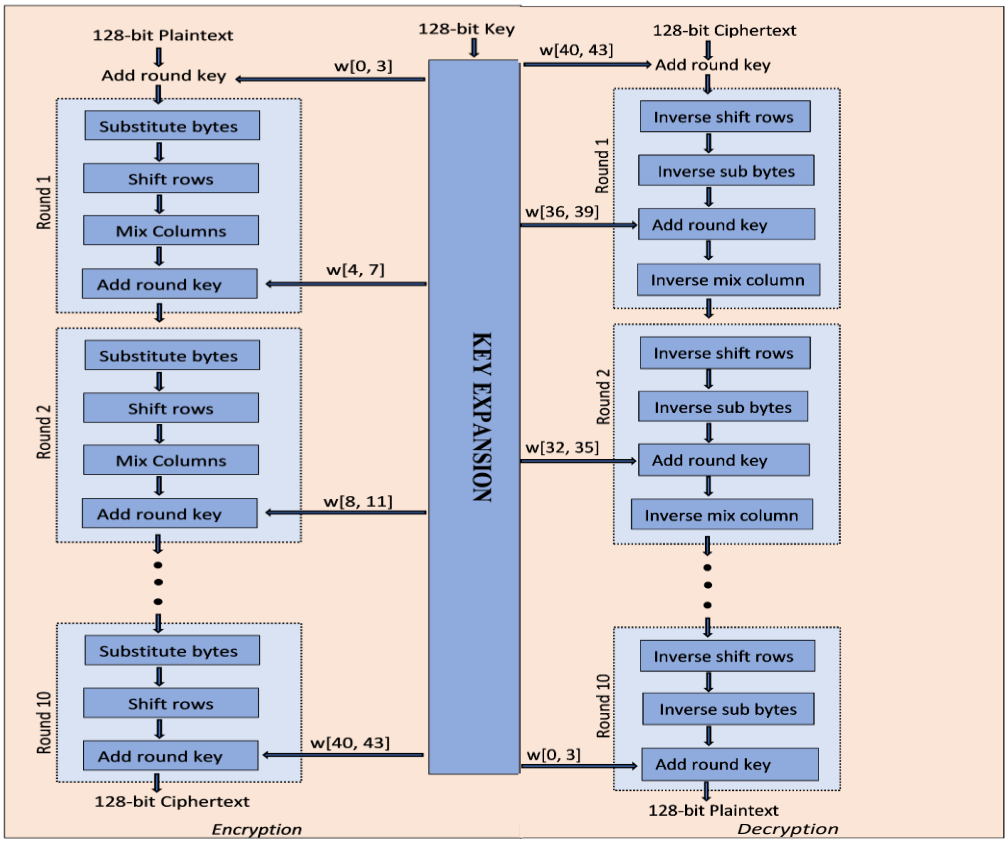


Fig. 2.1: AES Encryption and Decryption

The Ciência & Engenharia - Science & Engineering Journal
ISSN: 0103-944X
Volume 11 Issue 1, 2023
pp: 1841-1853

3.2 Substitute Bytes

The substitute bytes (Fig. 2.2)are referred to as SubBytes of the ciphers which use S-box (Table 1).A well-defined method to generate the S-box is given in [4] (page number 35-37). In this step, each byte of the state array is replaced by another byte according to the substitution table (or S-box). S-box is a bijection over $\{0,1\}^8$. There is only one S-box which is a 16×16 array and it is used for substituting all the bytes inthe state array and in each round. In Fig 2.2 we use hexadecimal values in place of $S_{i,j}$ for each i and j. Since $S_{1,1}=\{76\}$ then it means we replace this element with the 7th row and 6th column of the S-box. But if $S_{1,1}=116$ it is not in the hexadecimal, then we change it into an 8-bit binary digit and the leftmost 4-bit is used as a row value and the rightmost 4-bit is used as a column value.

A binary value of 116→01110101. Therefore, it maps to the 7th row and 5th column of the S-box i.e. 116 replaced by 9D.

Pictorial representation of SUBBYTES

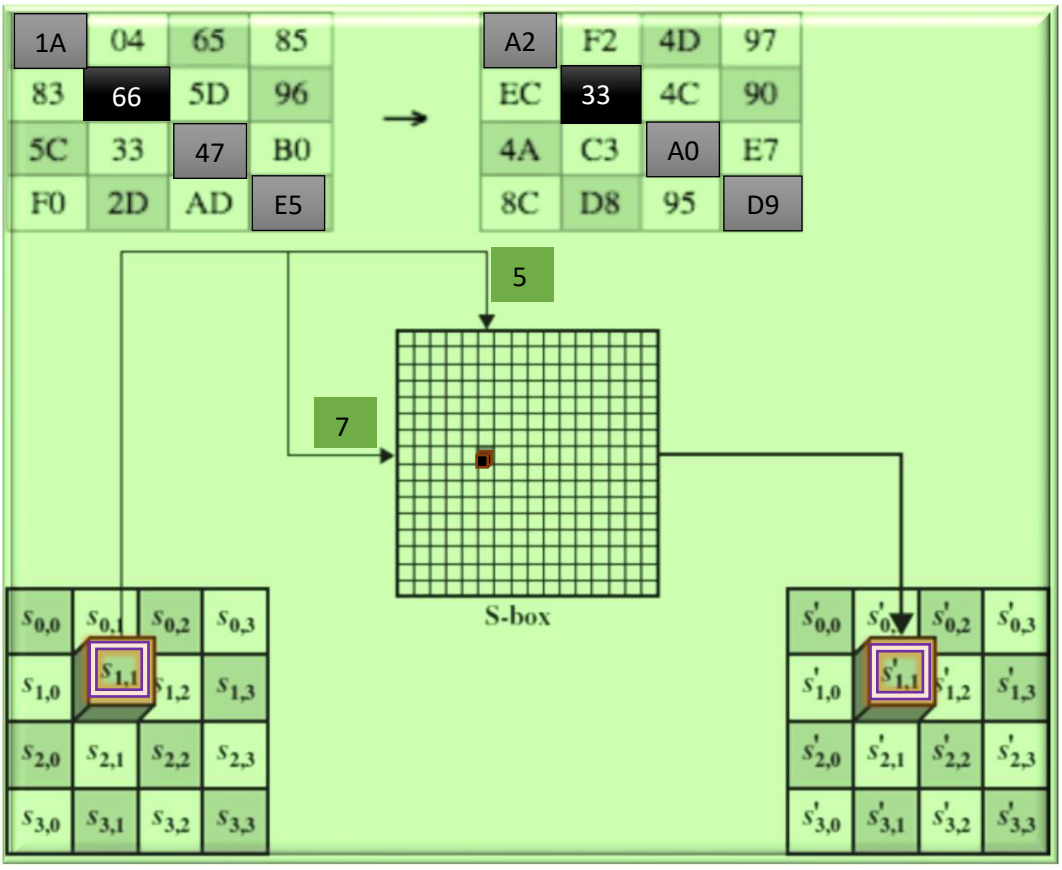


Fig. 2.2

The Ciência & Engenharia - Science & Engineering Journal
ISSN: 0103-944X
Volume 11 Issue 1, 2023
pp: 1841-1853

AES S-Box

	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

3.3 Shift Row

ShiftRow is the second step of each round performed in the AES encryption. The main idea behind this step is to shift bytes of the state cyclically to the left in each row except the row number zero. In this process, the bytes of row number zero remainthe same and do not carry out any permutation. In the first row, only one byte is shifted circularly to left,the second row is shifted two bytes to the left and the last row is shifted three bytes to the left. The size of the new state is not changed that remains the same as the original size of 16 bytes but shifted the position of the bytes in the state as illustrated in Fig. 2.3.

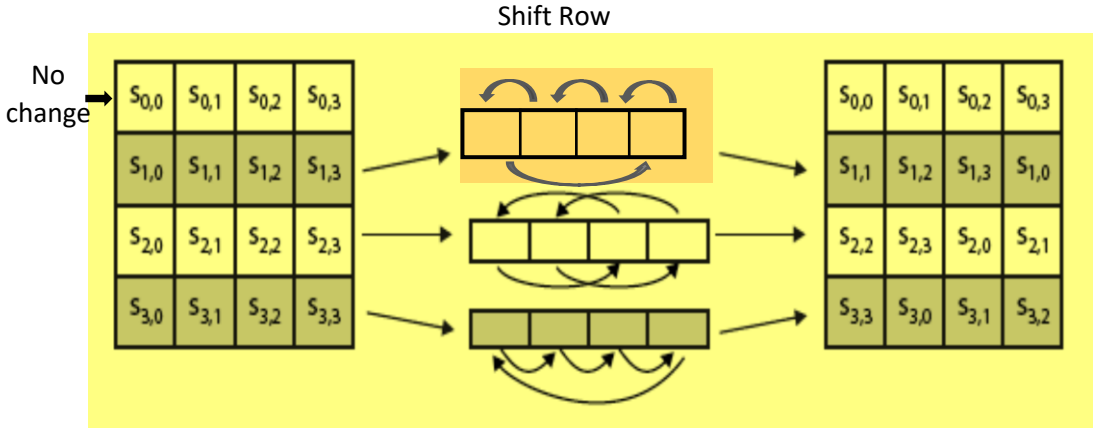


Fig. 2.3

The Ciência & Engenharia - Science & Engineering Journal
ISSN: 0103-944X
Volume 11 Issue 1, 2023
pp: 1841-1853

3.4 Mix Column

It is one of the critical steps in AES and is written as MixColumns. The multiplication is carried out of the state. Each byte of one row in matrix transformation multiply by each value (byte) of the state column. In another word, each row of matrix transformation must multiply by each column of the state. The results of this multiplication are used with XOR to produce a new four bytes for thenext state. In this step the size of the state is not changed that remained the same as the original size 4×4 as shown in Fig. 2.4.

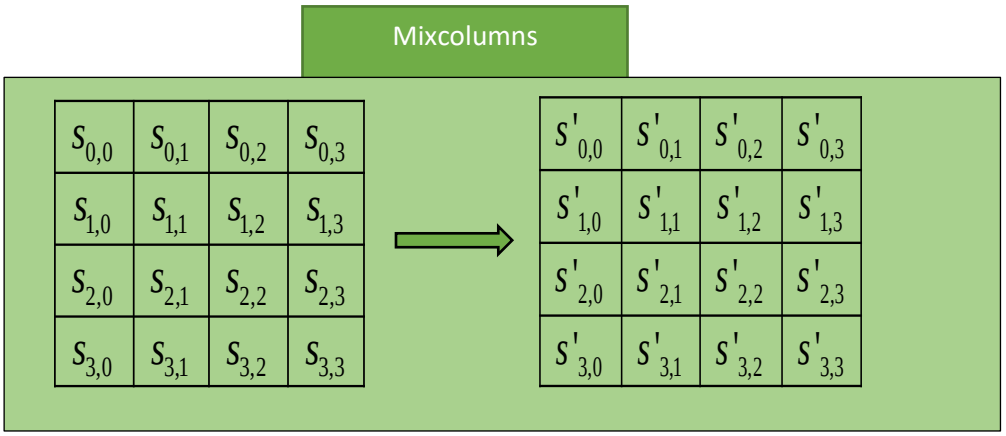


Fig. 2.4 The MixColumns transformation can be expressed as

$$s'_{0,j} = (x \cdot s_{0,j}) \oplus ((x+1) \cdot s_{1,j}) \oplus s_{2,j} \oplus s_{3,j}$$
$$s'_{1,j} = s_{0,j} \oplus (x \cdot s_{1,j}) \oplus ((x+1) \cdot s_{2,j}) \oplus s_{3,j}$$
$$s'_{2,j} = s_{0,j} \oplus s_{1,j} \oplus (x \cdot s_{2,j}) \oplus ((x+1) \cdot s_{3,j})$$
$$s'_{3,j} = ((x+1) \cdot s_{0,j}) \oplus s_{1,j} \oplus s_{2,j} \oplus (x \cdot s_{3,j})$$

3.5 Add Round Key

AddRoundKey is the most important stage in the AES algorithm and is referred as AddRoundKey. Both the key and the input dataare structured in a 4×4 matrix of bytes. Fig. 2.5 shows how the 128-bit key and input data are allocated into the byte matrices. AddRoundKeycan provide much more security during encrypting data. This operation is based on creating the relationship between the key and the ciphertext. The ciphertext is coming from the previous stage. The AddRoundKey output exactly relies on the key that is indicated by users. Furthermore, in the stage, the subkey is also used and combined with the state. The main key is used to derive the subkey in each round by using Rijndael's key schedule. The size of the subkey and state is same. The subkey is added by combining each byte of the state with the corresponding byte of the subkey using bitwise XOR.

The Ciência & Engenharia - Science & Engineering Journal
ISSN: 0103-944X
Volume 11 Issue 1, 2023
pp: 1841-1853

AddRoundKey

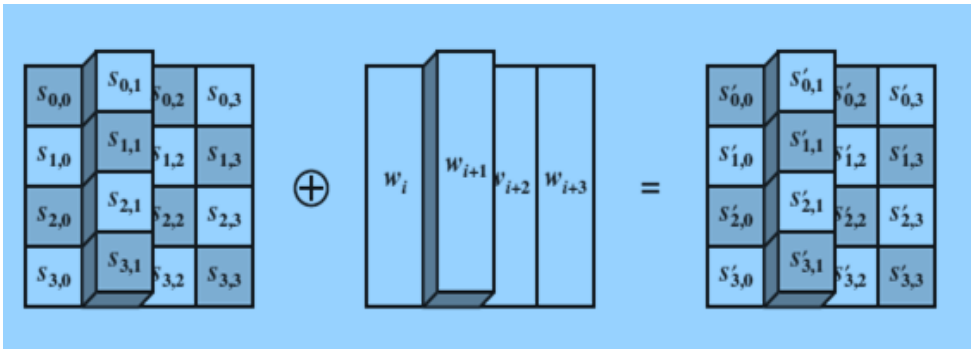


Fig. 2.5

3.6 Key Expansion Algorithm

The AES key expansion algorithm takes an input asa 128-bit (4 words i.e, 16 bytes) key and produces a linear array of 176 bytes (44 words). This is sufficient to provide a four-word round key for the initial AddRoundKey stage and each of the 10 rounds of the cipher. The key is copied into the first four words of the expanded key. The remainder of the expanded key is filled in four words at a time. Each added word $w[i]$ depends on the immediately preceding word $w[i-1]$ and the word four positions back $w[i-4]$. In three out of four cases, a simple XOR is used. For a word whose position in the w array is a multiple of 4, a more complex function is used. Fig.2.6 illustrates the generation of the expanded key, using the symbol g to represent that complex function.

I. RotWord performs a one-byte circular left shift on a word. This means that an input word $[B0, B1, B2, B3]$ is transformed into $[B1, B2, B3, B0]$.

II. SubWord performs a byte substitution on each byte of its input wordusing an S-box(Table-1).

III. The result of steps 1 and 2 is XORed with a round constant $Rcon[j]$.

The round constant is a word in which the three rightmost bytes are always 0. Thus, the effect of an XOR of a word with $Rcon$ is to only perform an XOR on the leftmost byte of the word. The round constant is different for each round and is defined $as\ Rcon[j] = (RC[j], 0, 0, 0)$, with $RC[1] = 1,\ RC[j] = 2 \cdot RC[j-1]$ and with multiplication defined over the field GF(2^8).

The Ciência & Engenharia - Science & Engineering Journal
ISSN: 0103-944X
Volume 11 Issue 1, 2023
pp: 1841-1853

Key Expansion Algorithm

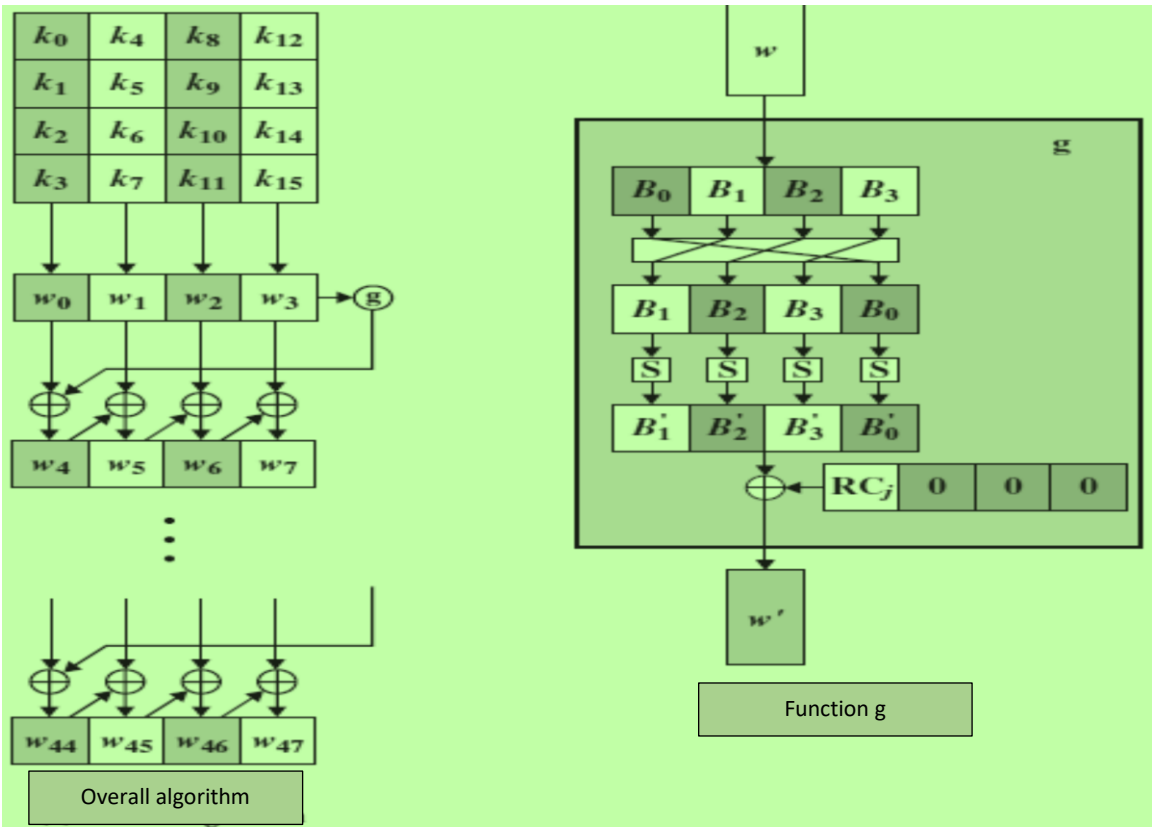


Fig.2.6

4.The Proposed Pseudorandom Number Generator (PRNG) Rc4-Gf

RC4 has a significant number of weaknesses, one of the reasons for these weaknesses is the initialization process in KSA. As it is a deterministic sequence giving the attackers a first-move advantage. So, we try to improve the initialization process of KSA of RC4 using the non-deterministic sequence. We are using multiplicative inverse of the elements of GF(7^3) for initialization and changing some steps in PRGA we get RC4-GF with more random data (Algorithm 1). We used multiplicative inverses of 256 elemental polynomials of GF (7^3) with respect to irreducible polynomial x^3+x^2+5x+1 over Z_7 (Table-2) in place of S-box and for the secret key (k) we take (Table-3) rest of 86 elemental polynomials. (below the polynomial x^2+5x+3 written in number form as 153 and $5x+3$written as 53).

Table-2

1, 4, 5, 2, 3, 6, 662, 203, 610, 231, 216, 325, 650, 331, 143, 105, 516, 340, 360, 154, 223, 134, 315, 301, 240, 352, 250, 554, 520, 425, 530, 406, 462, 643, 446, 623, 410, 430, 261, 602, 634, 115, 120, 452, 561, 546, 160, 504, 543, 221, 252, 123, 633, 22, 262, 466, 345, 511, 421, 202, 60, 651, 61, 326, 524, 103, 145, 465, 661, 615, 205, 363, 553, 31, 463, 140, 136, 163, 445, 21, 603, 124, 313, 255, 354, 500, 416, 26, 440, 456, 65, 204, 640, 141, 333, 533, 230, 625, 355, 114, 11, 161, 131, 415, 453, 305, 435, 412, 226, 545, 14, 233, 101, 526, 30, 644, 364, 214, 166, 13, 562, 220, 600, 263, 243, 34, 426, 513, 236, 612, 334, 405,

The Ciência & Engenharia - Science & Engineering Journal
ISSN: 0103-944X
Volume 11 Issue 1, 2023
pp: 1841-1853

36, 555, 102, 655, 320, 150, 424, 346, 54, 106, 235, 535, 420, 665, 461, 33, 531, 335, 323, 211, 343, 344, 660, 652, 146, 642, 32, 400, 254, 621, 441, 304, 560, 15, 121, 622, 20, 635, 164, 245, 303, 455, 24, 411, 565, 306, 310, 111, 260, 512, 536, 35, 521, 151, 201, 664, 25, 624, 501, 132, 225, 564, 436, 316, 434, 566, 454, 442, 246, 44, 52,341, 213, 552, 645, 206, 153, 265, 113, 506, 626, 256, 42, 241, 53, 510, 666, 460, 401, 212, 366, 155, 322, 404, 532, 613, 142, 50, 523, 656, 62, 210, 403, 336, 156, 433, 300, 45, 135, 631, 125, 110, 152, 362, 646, 616, 66, 663, 422, 431, 112, 350, 242, 542.

256MI of GF(7^3) with respect to irreducible polynomial x^3+x^2+5x+1

Table-3

601, 23, 41, 353, 620, 450, 122, 605, 222, 43, 302, 443, 165, 541, 264, 351, 611, 534, 514, 100, 550, 215, 64, 544, 563, 413, 133, 40, 251, 606, 324, 63, 232, 551, 365, 342, 402, 234, 515, 55, 144, 654, 525, 556, 12, 540, 244, 444, 636, 130, 503, 522, 321, 330, 51, 361, 200, 423, 641, 464, 653, 104, 56, 332, 614, 162, 630, 314, 46, 224, 414, 502, 16, 116, 312, 632, 604, 253, 451, 311, 126, 10, 505, 356, 266, 432

86MI of GF(7^3) with respect to irreducible polynomial x^3+x^2+5x+1 for key(k)

Input:
1. Secret key array K[0 . . . 99].
2. multiplicative inverse of polynomials m[0 1 . . . 255]
Output: Scrambled array S[0 . . . 255].
initialization
for i = 0 . . . 255 do
S[i] = mi;
j = 0;
Scrambling:
if i=even
j = (j + S[i] + K[i]);
Swap (S[i], S[j]);
Else;
j= (j + m[i](mod 256) + K[i]);
Swap (S[i], S[j]);
KSA
	Input: scrambled array S[0 . . . 255].
	Output: Pseudo-random keystream bytes.
	initialization
	i = j = 0;
	Output Keystream Generation Loop:
	i = i + 1;
	j =S[j + S[i + j]];
	Swap(S[i], S[j]);
	z = S[i + j] + S[j];
	Output = S[S[S[z]]+j];
	PRGA

Algorithm 1:RC4-GF KSA and PRGA

The Ciência & Engenharia - Science & Engineering Journal
ISSN: 0103-944X
Volume 11 Issue 1, 2023
pp: 1841-1853

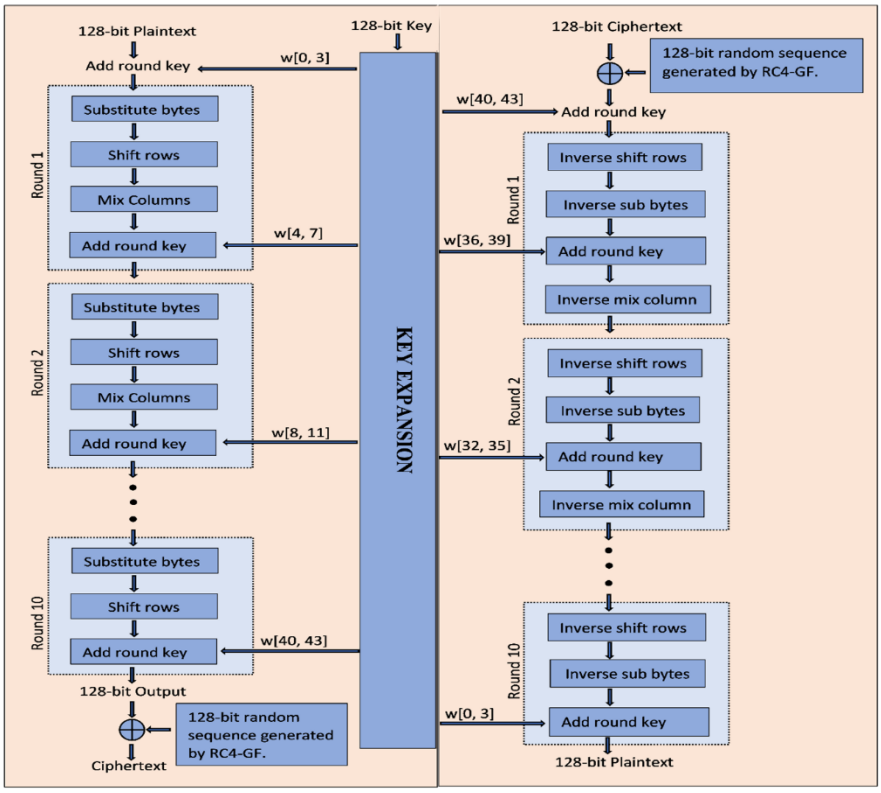
5. Modified Aes

Presently the advanced digital world always needs a new stronger version of AES better than the existing version. In this direction we combined both AES and RC4-GF to introduce a new type of encryption algorithm and named it AES-RC4.TheAES-RC4 is a symmetrical block cipher algorithm that also uses 128,192 or 256-bit keys to transform a block of 128 bits message into 128 bits of ciphertext because the key of AES-RC4 hasthe same number of bits as AES. AES-RC4 is a roundbased algorithm and the rounds of it depend on the key length as same as AES. In the encryption process the 128, 192 and 256-bit keys consist of 10, 12 and 14 rounds respectively.

The input state array is XORed with the first 128 bits of the key schedule before the rounds for encryption start. Each round except the last round consists of the following four steps for encryption:

Substitute bytes, Shift rows, Mix columns and Add round key,but the last round does not have the mix columns stepi.e, in the last round we XOR the four words (128-bit) from the key schedule with the output of the previous two steps (Substitute bytes and Shift rows). After that we XOR the first 128 bit of final output of RC4-GF and we get the cipher text of AES-RC4. During decryption, first we XOR the 128-bit final output of RC4-GFafter that weXOR the ciphertext state array with the last four key schedule words. Similarly, each round except the last consists of the following four steps for decryption:

Inverse shift rows, Inverse substitute bytes, Add round key and Inverse mix columns but the last round does not have the inverse mix columns step. Lastly we XOR the four words from the keyschedule with the output of the previous two steps (Fig.3).



6. Conclusion

In Section 1 of the present work, we introduced the encryption algorithm for plaintext and the research conducted by various researchers in this field. Sections 2 and 3 provided detailed overviews of the DES and AES encryption algorithms, respectively.In Section 4, the new variant of RC4named as RC4-GF has been discussedwhereas in section 5
a new variant of AES called AES-RC4 has been discussed. AES-RC4 is a combination of the AES algorithm and a specially designed encryption algorithm called RC4-GF. By integrating the strengths of both algorithms, AES-RC4 offers enhanced capabilities compared to AES alone.As a result, the ciphertext produced by AES-RC4 exhibits increased resistance against various types of cyber-attacks.

7. References

[1] D. Coppersmith, "The Data Encryption Standard (DES) and its strength against attacks," in IBM Journal of Research and Development, vol. 38, no. 3, pp. 243-250, May 1994, doi: 10.1147/rd.383.0243.

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

[3] Biham, Eli et al. “The Rectangle Attack - Rectangling the Serpent.” *International Conference on the Theory and Application of Cryptographic Techniques* (2001).

[4] J. Daemen and V. Rijmen, "The design of Rijndael: AES the advanced encryption standard", Springer-Verlag, 2002.

[5] Isa, Herman & Bahari, Iskandar &Sufian, Hasibah&Zaba, Muhammad. (2011). AES: Current security and efficiency analysis of its alternatives. Proceedings of the 2011 7th International Conference on Information Assurance and Security.

[6] Alalak, Saif&Zukarnain, Zuriati& Abdullah, Azizol&Subramiam, Shamala. (2013). Randomness improvement of AES using MKP. Research Journal of Information Technology. 5. 24-34. 10.3923/rjit.2013.24.34.

[7] Abdullah, Ako. (2017). Advanced Encryption Standard (AES) Algorithm to Encrypt and Decrypt Data.

[8] Kumar, A., Dhabliya, D., Agarwal, P., Aneja, N., Dadheech, P., Jamal, S. S., & Antwi, O. A. (2022). Research Article Cyber-Internet Security Framework to Conquer Energy-Related Attacks on the Internet of Things with Machine Learning Techniques.

[9] Dawood, Omar A. & Hammadi, Othman. (2017). An Analytical Study for Some Drawbacks and Weakness Points of the AES Cipher (Rijndael Algorithm). 10.25212/ICoIT17.013.

[10] Atikah, Nur &RizkyAshila, Mutia& Setiadi, De Rosal Ignatius Moses &Rachmawanto, Eko& Sari, Atika. (2019). AES-RC4 Encryption Technique to Improve File Security.

[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] Anand, R., Ahamad, S., Veeraiah, V., Janardan, S. K., Dhabliya, D., Sindhwani, N., & Gupta, A. (2023). Optimizing 6G Wireless Network Security for Effective Communication. In

Innovative Smart Materials Used in Wireless Communication Technology (pp. 1–20). IGI Global.

[13] Sousi, Ahmad-Loay&Yehya, Dalia &Joudi, Mohamad. (2020). AES Encryption: Study & Evaluation.

[14] J. Kaur, S. Lamba and P. Saini, "Advanced Encryption Standard: Attacks and Current Research Trends," 2021 International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE), Greater Noida, India, 2021, pp. 112-116, doi: 10.1109/ICACITE51222.2021.9404716.

[15] Pandey, J. K., Ahamad, S., Veeraiah, V., Adil, N., Dhabliya, D., Koujalagi, A., & Gupta, A. (2023). Impact of Call Drop Ratio Over 5G Network. In Innovative Smart Materials Used in Wireless Communication Technology (pp. 201–224). IGI Global.

[16] K. Janshi Lakshmi, G. Sreenivasulu, "A Review on FPGA Based Design of Advanced Encryption Standard (AES) Cryptography Secure Algorithm", *i-manager's Journal on Communication Engineering and Systems*, vol.10, no.1, pp.30, 2021.

[17] S. Muthusundari, A. Sonya, C. M. Nalayini, A. R. Sathyabama, P. V. Rajasuganya, "Safe Encryption Algorithm for Secured Message Communication Using Dcombo: A New Sorting Technique", *Proceedings of Second International Conference on Sustainable Expert Systems*, vol.351, pp.559, 2022.

[18] Talukdar, V., Dhabliya, D., Kumar, B., Talukdar, S. B., Ahamad, S., & Gupta, A. (2022). Suspicious Activity Detection and Classification in IoT Environment Using Machine Learning Approach. 2022 Seventh International Conference on Parallel, Distributed and Grid Computing (PDGC), 531–535. IEEE.