Comparative Analysis of Reduced Round Dynamic AES with Standard AES Algorithm

Amandeep Singh
Department of Computer Science
Baba Farid College
Bathinda - 151001

ABSTRACT
Block ciphers are built around the substitution table, or S-Box. The cipher's protection is improved by better-designed S-Boxes. The Advanced Encryption Algorithm is already a formidable algorithm with excellent linear and differential properties. To provide more security and complexity to standard AES algorithm a dynamic AES with key dependent dynamic S-Boxes developed for each round of dynamic AES. In this study reduced round (RR) variant of dynamic AES with 8 round of encryption is investigated. The aim of this study is to compare the reduced round (RR) variant of dynamic AES with standard AES on the basis of the criterion SAC (strict avalanche criterion) and BIC (bit independence criterion), which further tests the non-linearity and randomness of cipher text on which the security of algorithms is based.

General Terms
Standard AES, Reduced Round Dynamic AES, Dynamic S-Box, SAC, BIC, AES Security.

Keywords
Standard AES, Reduced Round Dynamic AES, Dynamic S-Box, SAC, BIC.

1. INTRODUCTION
AES is a block cipher widely used for encryption and decryption of data. AES block cipher was adopted by the US government as standard in 2001. Joan and Vincent Rijmen [1] developed AES block cipher AES uses block sizes of 128 bits for encryption at one time, which is fixed. AES has three variants in which variable key sizes for different rounds (10, 12, and 14) are used. AES uses three variants.

1. 128 bit key size for 10-round encryption
2. 192 bit key size for 12-round encryption
3. 256 bit key size for 14-round encryption

All the calculations of AES block cipher are carried out in finite fields, that is, GF(2^8). To encrypt the 128 bit input block with 128 bit key, 10-rounds are used each round consists of four possessing steps except the last round which consists only three steps. For decryption, same rounds and steps are used, but in reverse order. Different steps which are used in each round are as follows:

The substitution byte transformation: Substitution byte is a non-linear confusion process, which substitutes bytes of plain text (4×4 matrix) with the bytes of predefined AES S-Box. AES S-Box is a matrix of 256 elements (16×16 matrix) ranging from 0 to 255. S-Box values are computed using $Y = Ax \oplus C \; mod \; M$, where x is input byte, A is 8×8 affine matrix and $C$is affine constant i.e 63 and $M$is irreducible polynomial i.e. $x^8 + x^4 + x^3 + x + 1$. All elements of S-Box are mapped to its multiplicative inverse in $GF(2^8)$, where element 0 is mapped to itself. In decryption process AES inverse S-Box is used. AES S-Box is displayed in Table 1 and Figure 1 shows substitution byte process.

Table 1. 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	4	c7	23	c3	18	96	5	9a	7	12	80	e2	eb	27	b2	75
4	9	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	2	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	6	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	8
C	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
D	70	3e	b5	66	48	3	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

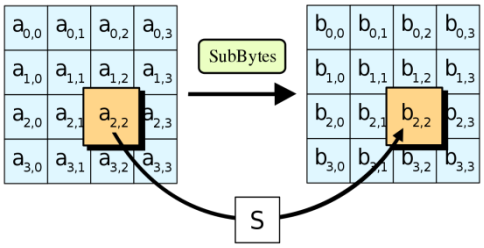

Fig 1: Byte Substitution

Shift row transformation: Shift row is a 4 x 4 matrix linear diffusion method that works on individual rows. The first row of the matrix remains unchanged, the second row has one left shift, the third row has two left shifts, and the fourth row has three left shifts. Shift row in presented in Figure 2.

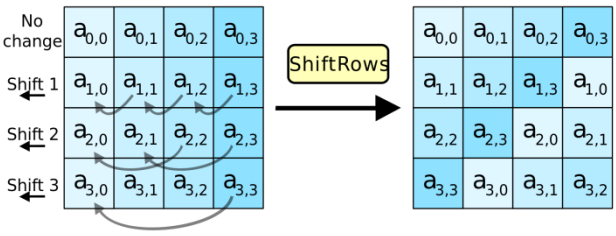

Fig 2: Shift Rows

Mix column transformation: in mix column transformation matrix multiplication is done over GF(2^8). Multiplication of

column vector is done with a fixed matrix, where all the bytes are treated as polynomials. Mix column is presented in Figure 3.

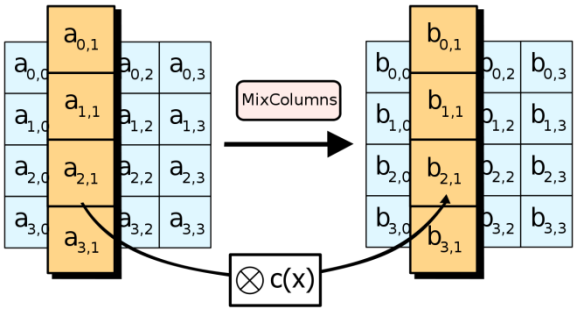

Fig 3: Mix Column

Add round key: At last bytes of round key are XORed with bytes of state matrix

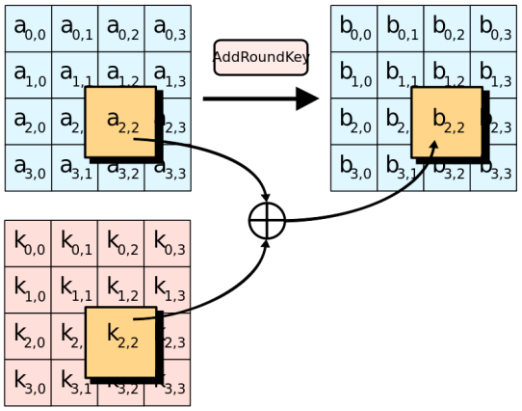

Fig 4: Add Round Key

2. RELATED WORK

The substitution box, also known as the S-Box, is the only non-linear part of block cipher AES that provides the confusion property. The strength of these block ciphers is largely determined by the nature of S-Boxes in cryptography. The S-Boxes should be secure enough to withstand various algebraic attacks cryptographically. AES is a very powerful algorithm, but one of its drawbacks is that it uses a fixed S-Box in all of the encryption rounds, which could contribute to cryptanalysts.

GN Krishnamurthy and V Ramaswamy [2] used AES-KDS block cipher, in which they used S-Box rotation on each round. They also used different stages to enhance the security. Piotr Mroczkowski [3] used pseudorandom sequences to generate identical boxes for encryption and decryption. Abd-ElGhafar et. al [4] used RC4 algorithm to generate key dependent dynamic S-Boxes. All values of S-Box are based on input key, when any byte of key is changed then all 256 values were permuted. Ghada Zaibi et. al [5] presented one-dimensional chaotic maps algorithm to construct a dynamic S-Boxes. Jie Cui et. al [6] modified affine transformation of AES algorithm and generated dynamic S-Boxes. Julia Juremi et. al [7] presented key expansion algorithm along with S-box rotation to make S-Box key dependant. Mona Dara et. al [8] used Chaotic Logistic Map to generate S-box for AES using its cipher key. Eman Mohammed Mahmoud et. al [9] used PN Sequence generator to generate random sequence of bits. LFSR (Linear Feedback Shift Register) technique used to generate key dependent dynamic S-Boxes. Fatma Ahmed et. al [10] used S-boxes bank like a rotor mechanism and dynamic key MDS matrix (SDK-AES) to generate dynamic S-Boxes. Adi Narayana Reddy K et. al [11] added a secrete value to the static index to shift the substitution to a secrete location and also generated variable sub keys by using sequence of pseudo random numbers to generate dynamic S-Boxes. Kazlauskas et. al [12] improvised their key dependent S-Box algorithm to make it efficient. Balajee Maram et. al [13] used Pseudo-Random generator and proposed a new algorithm to generate dynamic S-Boxes.

3. SECURITY OF AES

Although, AES is a very strong and immune to algebraic attacks. There are various attacks formulated by cryptanalysts on various round of AES known as Square attack.

Lars Knudsen invented the square attack for the reduced round variant of AES, and it was extended to a block cypher square for the first time [14]. It's a plain text attack that has been specifically selected. In this attack, the attacker breaks a block cipher's substitution permutation network (SPN) by using a carefully chosen collection of plaintexts and multisets, where multisets refers to a group of values that appear multiple times in the cipher. This attack was originally designed to target four rounds of 128-bit AES [15], but it was later expanded to six rounds to target 192-bit and 256-bit AES. For all versions of AES (128, 192, and 256), an improved 7-round attack was implemented. The seven-round attack, on the other hand, was slower [16]. On the 192 and 256 bit versions of AES, an additional 8-round attack was implemented, which was practically infeasible [17].

On observing immunity of AES against reduced round attacks a modified Reduced Round Dynamic AES is proposed and results are also compared with standard AES algorithm.

4. PROPOSED REDUCED ROUND DYNAMIC AES ALGORITHM

The proposed Reduced Round Dynamic AES is the reduced variant of Dynamic AES which uses 8 rounds to encrypt plain text. This algorithm uses 128 bit block of information and 128 bit key for encryption and decryption. This algorithm uses dynamic S-Box construction presented in Figure 5. for added security and complexity [20]. RR Dynamic AES uses 8 rounds for encryption and decryption in which 7 rounds of encryption process includes byte substitution, shift row, mix column and add round key and 8th round uses only three transformations except mix column. Reduced Round Dynamic Algorithm encryption and decryption is presented in Figure 6 and Figure 7 respectively.

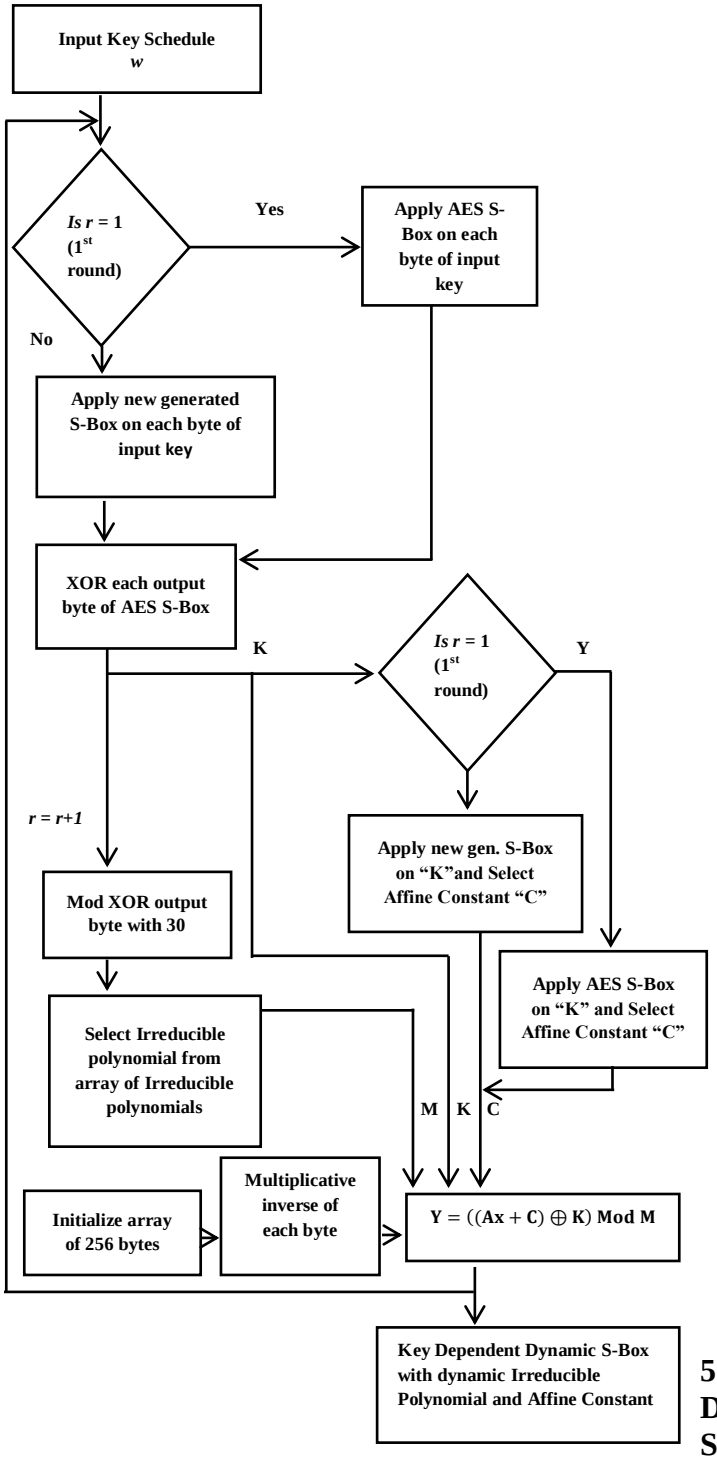

Fig 5: Flow Chart of Key Dependent Dynamic S-Box Generation

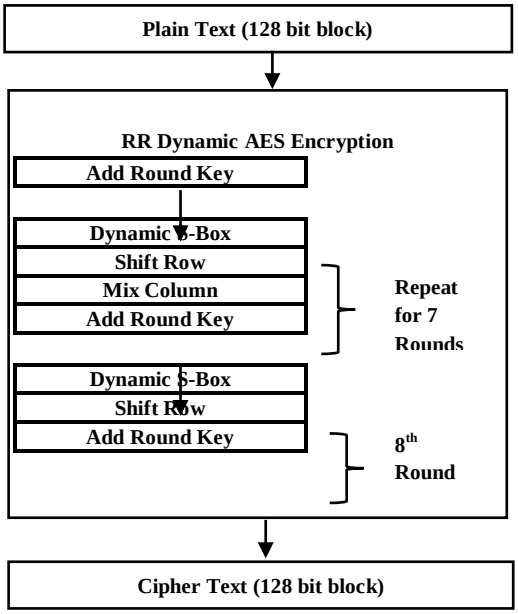

Fig 6: RR Dynamic Encryption Algorithm

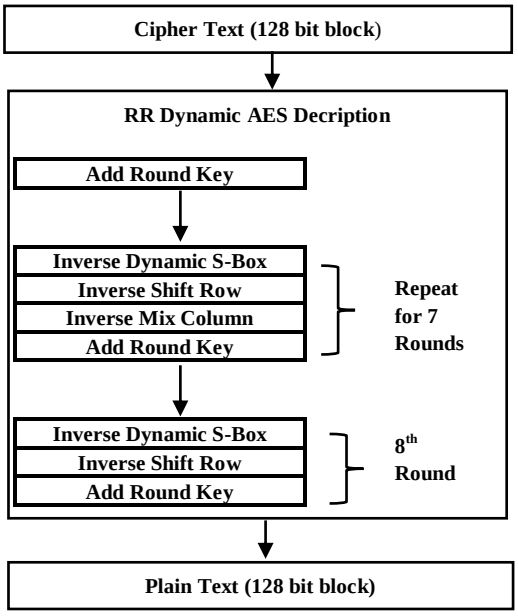

Fig 7: RR Dynamic Decryption Algorithm

5. ANALYSIS OF REDUCED ROUND DYNAMIC AES IN COMPARISON WITH STANDARD AES

On the basis of criteria such as SAC and bit independence criterion, the RR Dynamic S-Box is analyzed and compared to standard AES

5.1 Strict Avalanche Criteria (SAC)

Webster and Tavares [18] introduced the Strict Avalanche Criterion (SAC). When a single bit of plain text or a key is complemented, each of a function's output bits should change with a probability of one half, according to the strict avalanche criterion.

$$\alpha = \sum_{x \in Z_2^n} f(x) \oplus f(x \oplus e_i), \qquad (1)$$

Where, x and e are two n-bit vectors that only differ in one bit i. The Boolean function $f(x)$ accomplishes SAC criterion if and only if $\alpha = 2^{n-1}$ for $all\ i, 0 \leq i \leq n-1$.

Strict avalanche criterion will be presented both by changing one bit change in plain text and key respectively. Following are the plain texts and keys used for this test in Table 2 and Table 3 respectively.

Table 2. Plain text with one bit change

Plain Texts	Change on Bit Positions	Plain Text
Plain Text 1	0	3243F6A8885A308D313198A2E0370734
Plain Text 2	2	7243F6A8885A308D313198A2E0370734
Plain Text 3	4	6243F6A8885A308D313198A2E0370734
Plain Text 4	8	6343F6A8885A308D313198A2E0370734
Plain Text 5	16	3242F6A8885A308D313198A2E0370734
Plain Text 6	32	3243F6A9885A308D313198A2E0370734
Plain Text 7	64	3243F6A8885A308C313198A2E0370734
Plain Text 8	128	3243F6A8885A308D313198A2E0370735

Table 3. Key with one bit change

Key	Change on Bit Positions	Keys
Key 1	0	00E9C9F2A509D4E8A8BBB760A02AAB08
Key 2	1	80E9C9F2A509D4E8A8BBB760A02AAB08
Key 3	2	40E9C9F2A509D4E8A8BBB760A02AAB08
Key 4	3	20E9C9F2A509D4E8A8BBB760A02AAB08
Key 5	4	10E9C9F2A509D4E8A8BBB760A02AAB08
Key 6	5	08E9C9F2A509D4E8A8BBB760A02AAB08
Key 7	6	04E9C9F2A509D4E8A8BBB760A02AAB08
Key 8	7	02E9C9F2A509D4E8A8BBB760A02AAB08
Key 9	8	01E9C9F2A509D4E8A8BBB760A02AAB08

5.1.1 SAC with one bit change in plain text using different keys

RR Dynamic AES and standard AES are tested by encrypting plain text with single bit change in plain text at various bit positions with different keys to see the performance of RR Dynamic AES and standard AES. The plain texts used for analysis are presented in table 2. Table 4 compares the encrypted plain text and SAC values of RR Dynamic AES and standard AES with single bit change in plain text at various bit positions by using key 1. The results are vary comparative as standard value of SAC should be around 50%.

While keeping in view of length of article all encrypted plain texts with key 1 to key 9 are summarized in Table 5 and average SAC is presented graphically in Figure 8.

Table 5 presents results of SAC after encrypting plain texts with various keys. Here it is clearly represented that performance of RR Dynamic AES and standard AES is very comparable. Performance of RR Dynamic AES in Average SAC value for key 1, key 2, key 6 and key 8 is better than standard AES and for key 7 and key 9, there is slight difference of 0.2% only. Overall SAC value of all encrypted plain texts of RR Dynamic AES and standard AES is 49.37% and 49.40% respectively, which shows RR Dynamic AES is slightly more efficient even with reduced rounds, but with added complexity, which make cryptanalysis more difficult. The graphical representation is given in Figure 8.

Table 4. SAC of RR Dynamic AES and standard AES with single bit change in plain text using Key 1

Change on Bit Pos. in Plain Text	Plain Text	AES Cipher	RR Dyn. AES	AES SAC	RR Dyn. AES SAC
0	3243F6A8885A308D 313198A2E0370734	14CC5672E40E471A 50339F88BE73B60B	E153D379983FC090 CFDEB0BBED5928D9	-	-
2	7243F6A8885A308D 313198A2E0370734	83084421243C63F8 660A4A1A3144AC9C	AEC52C92FB207B14 0EF3EFE95E4161D5	46.1	53.1
4	6243F6A8885A308D 313198A2E0370734	85D5FE21B466A0AA F4 B6A35E5335FFA1	632FB5357262CA36 32E7E4146DBDD43E	45.3	52.3
8	6343F6A8885A308D 313198A2E0370734	EC9DF3A95988A03B F8 082E28B3E69187	0FF2AA7A73BBB9B4 2444722D3D775B51	49.2	48.4
16	3242F6A8885A308D 313198A2E0370734	A21393866FC99B47 408EE199B56196C3	E0D7F0287CD11323 F5 95E7AA3C18041E	50.0	45.3
32	3243F6A9885A308D 313198A2E0370734	5FA123555E4D3491D 3CCA9A8287C6EED	7FDCE207D8A98926 6175B54C6C6C09A8	53.1	49.2
64	3243F6A8885A308C 313198A2E0370734	618F9764D457CA9C 993A70113437DC57	5ACC3E09A1BF4558 66B3FB458F6032DB	44.5	49.2
128	3243F6A8885A308D 313198A2E0370735	0640A46FB1BB100F 52BB1B421DE456FA	9090A0BA39A16A09 F0F47ACC70613547	44.5	53.9

Table 5. Average SAC of RR Dynamic AES and standard AES with single bit change in plain text

	Key 1		Key 2		Key 3		Key 4		Key 5		Key 6		Key 7		Key 8		Key 9	
Plain Text	**AES**	**RR Dyn AES**	**AES**	**RR Dyn AES**	**AES**	**RR Dyn AES**	**AES**	**RR Dyn AES**	**AES**	**RR Dyn AES**	**AES**	**RR Dyn AES**	**AES**	**RR Dyn AES**	**AES**	**RR Dyn AES**	**AES**	**RR Dyn AES**
Plain Text 1	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Plain Text 2	46.1	53.1	52.3	50.8	51.6	43.8	50.8	54.7	53.9	51.6	50.0	53.1	52.3	53.1	53.9	47.7	46.1	51.6
Plain Text 3	45.3	52.3	50.0	55.5	53.1	57.0	54.7	51.6	47.7	47.7	53.1	50.8	50.0	50.8	52.3	53.1	51.6	53.1
Plain Text 4	49.2	48.4	49.2	44.5	52.3	41.4	57.8	53.9	46.1	46.1	47.7	57.0	53.9	50.0	49.2	45.3	50.0	49.2
Plain Text 5	50.0	45.3	50.0	56.3	51.6	45.3	51.6	46.1	47.7	52.3	45.3	58.6	57.0	55.5	54.7	57.8	50.8	43.8
Plain Text 6	53.1	49.2	50.8	51.6	55.5	52.3	49.2	50.8	48.4	49.2	45.3	56.3	50.0	48.4	52.3	53.9	51.6	45.3
Plain Text 7	44.5	49.2	46.1	47.7	52.3	57.8	53.9	43.8	54.7	42.2	46.1	44.5	45.3	49.2	54.7	57.0	51.6	59.4
Plain Text 8	44.5	53.9	49.2	43.0	53.1	47.7	47.7	53.1	44.5	46.9	50.0	44.5	47.7	47.7	49.2	53.9	48.4	46.1
Average	47.5	50.2	49.7	49.9	52.8	49.3	52.2	50.6	49.0	48.0	48.2	52.1	50.9	50.7	52.3	52.7	50.0	49.8

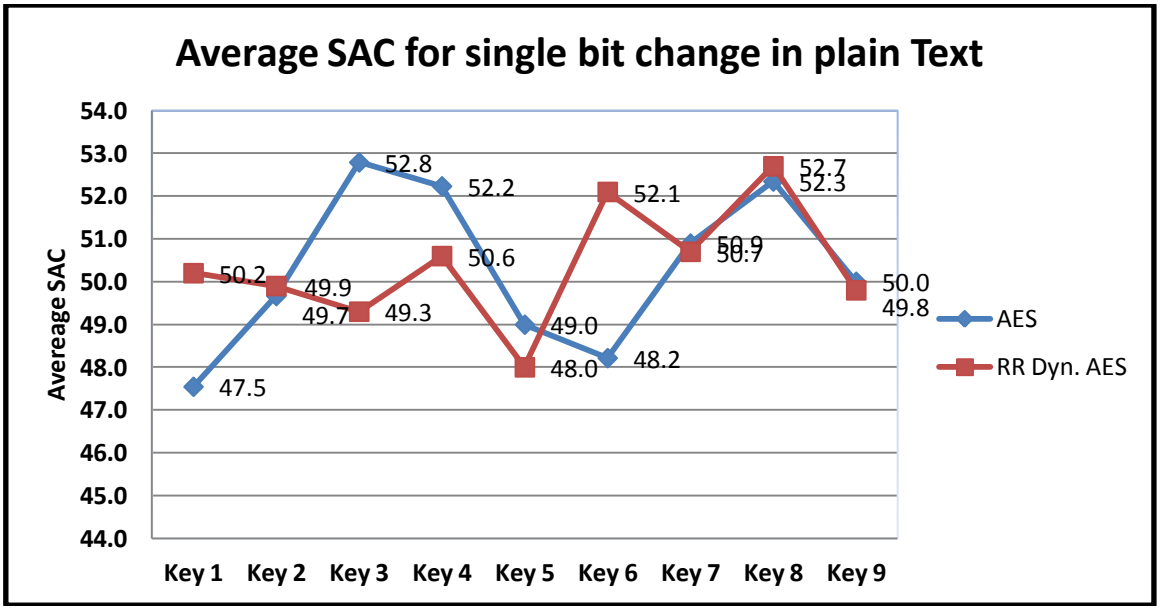

Fig 8: Graphical representation of Average SAC of RR Dynamic AES and Standard AES with one bit change in plain text

5.1.2 SAC with one bit change key using different plain texts

RR Dynamic AES and standard AES are tested by encrypting plain texts with single bit change in key at various bit positions to see the performance of RR Dynamic AES and standard AES. Keys used for analysis are presented in Table 3. Table 6 compares the encrypted plain text and SAC values of RR Dynamic AES and standard AES with single bit change in key at various bit positions by using plain text 1. The results are vary comparative as standard value of SAC should be around 50%.

While keeping in view of length of article all encrypted plain texts with single bit change in key are summarized in table 7 and average SAC is presented graphically in figure 4.

Table 6 presents results of SAC after encrypting plain texts with single bit change in key. Results here too of RR Dynamic AES and standard AES are very comparable. Performance of RR Dynamic AES in Average SAC value for plain text 3, 4, 6 and 8 is better than standard AES and for plain text 2, there is slight difference of 1% only. Overall SAC value of all encrypted plain texts of RR Dynamic AES and standard AES is 50.35% and 50.30% respectively, which shows RR Dynamic AES is slightly more efficient. The graphical representation is given in Figure 9.

Table 6. SAC of RR Dynamic AES and standard AES with single bit change in Key using Plain Text 1

Change on Bit Pos. in Key	Key	AES Cipher	RR Dyn. AES Cipher	AES SAC	RR Dyn. AES SAC
0	00E9C9F2A509D4E8A 8BBB760A02AAB08	14CC5672E40E471A 50339F88BE73B60B	E153D379983FC090C FDEB0BBED5928D9	-	-
1	80E9C9F2A509D4E8A 8BBB760A02AAB08	CF768BA0BF045FCE 840D9F7AD546A0C8	A23F94337B5BC179 9A30E2FF4D0322FF	50.0	42.2
2	40E9C9F2A509D4E8A 8BBB760A02AAB08	5FB6A8A237FB18F3 DD415B7B1E693754	E962CA5EC465A38E 1C43F03C46E3D4BD	55.5	47.7
3	20E9C9F2A509D4E8A 8BBB760A02AAB08	BF1486001C3FEC351 CA5F9DED62CE1E8	8F12D286E8F70CA5 0ACAFA79B50C7DE3	53.1	44.5
4	10E9C9F2A509D4E8A 8BBB760A02AAB08	644C99563CE89184 E7B818141C0ACC34	BF174EBFC4F33BB8 7A07F430F889D51B	53.1	50.8
5	08E9C9F2A509D4E8A 8BBB760A02AAB08	3D56B7CB1306079B EFDBB805D83FC30B	F9C672C71A873D21 050873B2C7EF3F26	45.3	52.3
6	04E9C9F2A509D4E8A 8BBB760A02AAB08	7D9E8E986215ECDF ABDAF5B850202B6D	2AFE42418F4C5F6D C36BEDB638DEB902	53.9	55.5
7	02E9C9F2A509D4E8A 8BBB760A02AAB08	1C69CD770C733AE2 AD3BA72B4431B694	D49CEB8D7AB8EA14 56939B399FE5A9E4	48.4	47.7
8	01E9C9F2A509D4E8A 8BBB760A02AAB08	7CD3E5A4249DDE81 B80944FBA806E34F	ECBDFC0C4ABD1FA 1F14748D7A8EF0A3C	51.6	53.1

Table 7. Average SAC of RR Dynamic AES and standard AES with single bit change in key

	Plain Text 1		Plain Text 2		Plain Text 3		Plain Text 4		Plain Text 5		Plain Text 6		Plain Text 7		Plain Text 8	
Keys	**AES**	**RR Dyn. AES**	**AES**	**RR Dyn. AES**	**AES**	**RR Dyn. AES**	**AES**	**RR Dyn. AES**	**AES**	**RR Dyn. AES**	**AES**	**RR Dyn. AES**	**AES**	**RR Dyn. AES**	**AES**	**RR Dyn. AES**
Key 1	-	-	-	-	-	-	-	-	-	-	-		-	-	-	-
Key 2	50.0	42.2	50.0	47.7	51.6	53.1	53.1	55.5	54.7	48.4	49.2	49.2	56.3	56.3	54.7	48.4
Key 3	55.5	47.7	53.1	55.5	49.2	52.3	49.2	57.8	49.2	44.5	43.8	55.5	46.1	48.4	46.9	53.9
Key 4	53.1	44.5	48.4	47.7	43.8	53.1	46.1	51.6	45.3	50.0	47.7	47.7	59.4	42.2	42.2	53.1
Key 5	53.1	50.8	43.8	52.3	53.9	52.3	50.0	42.2	49.2	50.0	51.6	50.8	43.0	51.6	43.8	50.0
Key 6	45.3	52.3	57.0	52.3	59.4	46.1	46.9	50.0	51.6	45.3	48.4	50.0	53.1	50.8	55.5	60.2
Key 7	53.9	55.5	49.2	47.7	49.2	47.7	47.7	52.3	51.6	51.6	49.2	43.8	48.4	44.5	41.4	44.5
Key 8	48.4	47.7	43.8	45.3	49.2	51.6	43.8	47.7	43.8	43.0	49.2	43.0	49.2	47.7	48.4	49.2
Key 9	51.6	53.1	46.9	34.4	42.2	47.7	47.7	50.8	60.2	51.6	50.0	49.2	49.2	50.8	41.4	48.4
Average	**51.4**	**49.2**	**49.0**	**47.9**	**49.8**	**50.5**	**48.0**	**51.0**	**50.7**	**48.0**	**48.6**	**48.6**	**50.6**	**49.0**	**46.8**	**51.0**

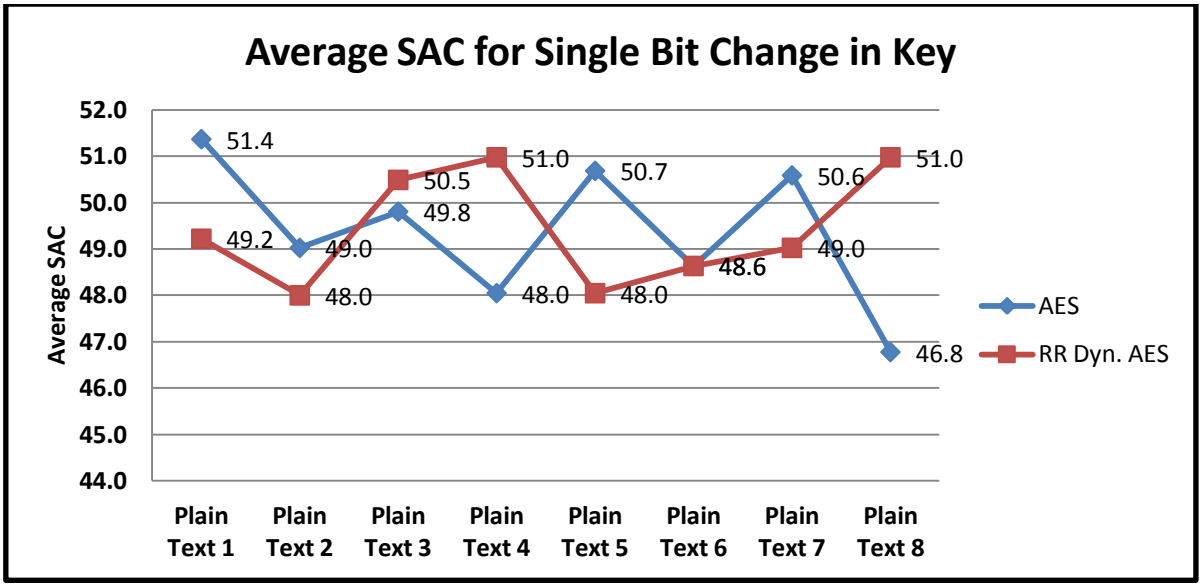

Fig 9: Graphical representation of Average SAC of RR Dynamic AES and Standard AES with one bit change in key

6. BIT INDEPENDENCE CRITERIA

Webster and Tavares [18] were the first to introduce the concept of BIC. All avalanche variables should be pair wise independent for a given set of avalanche vectors generated by changing a single bit of plain text or key. Bit independence property is measured by calculating correlation coefficient of j^{th} and k^{th} components of avalanche vector Dei over all input pairs P and Pi, which differ only in bit i ($P_i = P \oplus e_i$).

$$BIC^{e_i}(d_j, d_k) = \left| corr\left(d_j^{e_i}, d_k^{e_i}\right)\right|. \quad (2)$$

Then the overall BIC is defined as:

$$BIC(f) = \max_{1\le i\le n, 1\le j,k\le m, j\neq k} BIC^{e_i}(d_j, d_k). \quad (3)$$

$BIC(f)$ is a function that has a range of -1 to 1. It should ideally be equal to zero, and in the worst-case scenario, it should be equal to one

According to the BIC property, all the variables of a collection of avalanche vectors created by complementing a single bit of plain text should be pair-wise independent. To investigate this, the avalanche variable's correlation coefficient must be determined. The correlation coefficient has a value of between 1 and -1. If the correlation value is 0, the variables are independent and have no correlation; if the correlation value is 1, the variables have a strong positive correlation and if the correlation value is -1, the variables have a strong negative correlation. As a result, table 7 shows the correlation coefficient of AES and RR Dynamic AES when one bit of the plain is changed. Table 8 presents results of BIC after encrypting plain texts with various keys. RR Dynamic AES performs better as compared to standard AES for keys 2, 3, 4 ,6 ,7 and 9. Overall BIC for RR Dynamic AES and standard AES is 0.1885 and 0.2072. So here RR Dynamic AES is more efficient as com- pared to standard AES, which is more close to 0. The graphical representation is given in Figure 10.

Table 8. Correlation coefficient of avalanche vectors of AES and RR Dynamic AES

Plain Text	Key 1		Key 2		Key 3		Key 4		Key 5		Key 6		Key 7		Key 8		Key 9	
	RR Dyn. AES	AES	RR Dyn. AES	AES	RR Dyn. AES	AES	RR Dyn. AES	AES	RR Dyn. AES	AES	RR Dyn. AES	AES	RR Dyn. AES	AES	RR Dyn. AES	AES	RR Dyn. AES	AES
Plain Text 1	0.235	0.435	0.090	0.152	0.230	0.581	0.188	0.288	0.250	0.043	0.152	0.022	0.023	0.189	0.161	0.058	0.181	0.418
Plain Text 2	0.023	0.082	0.029	0.045	0.180	0.398	0.111	0.246	0.277	0.468	0.079	0.124	0.297	0.173	0.182	0.008	0.121	0.061
Plain Text 3	0.517	0.085	0.032	0.160	0.079	0.009	0.100	0.348	0.262	0.183	0.148	0.102	0.225	0.001	0.299	0.365	0.113	0.087
Plain Text 4	0.223	0.217	0.112	0.195	0.296	0.026	0.169	0.337	0.089	0.128	0.312	0.690	0.014	0.013	0.091	0.156	0.453	0.239
Plain Text 5	0.201	0.189	0.114	0.076	0.184	0.415	0.220	0.343	0.352	0.084	0.241	0.247	0.278	0.135	0.013	0.158	0.310	0.502
Plain Text 6	0.085	0.235	0.375	0.318	0.272	0.288	0.251	0.281	0.294	0.491	0.195	0.109	0.301	0.409	0.306	0.028	0.151	0.104
Plain Text 7	0.295	0.168	0.187	0.067	0.240	0.056	0.008	0.099	0.340	0.187	0.077	0.112	0.099	0.537	0.058	0.273	0.089	0.010
Average	0.225	0.201	0.134	0.145	0.212	0.253	0.150	0.278	0.266	0.226	0.172	0.201	0.177	0.208	0.159	0.149	0.203	0.203

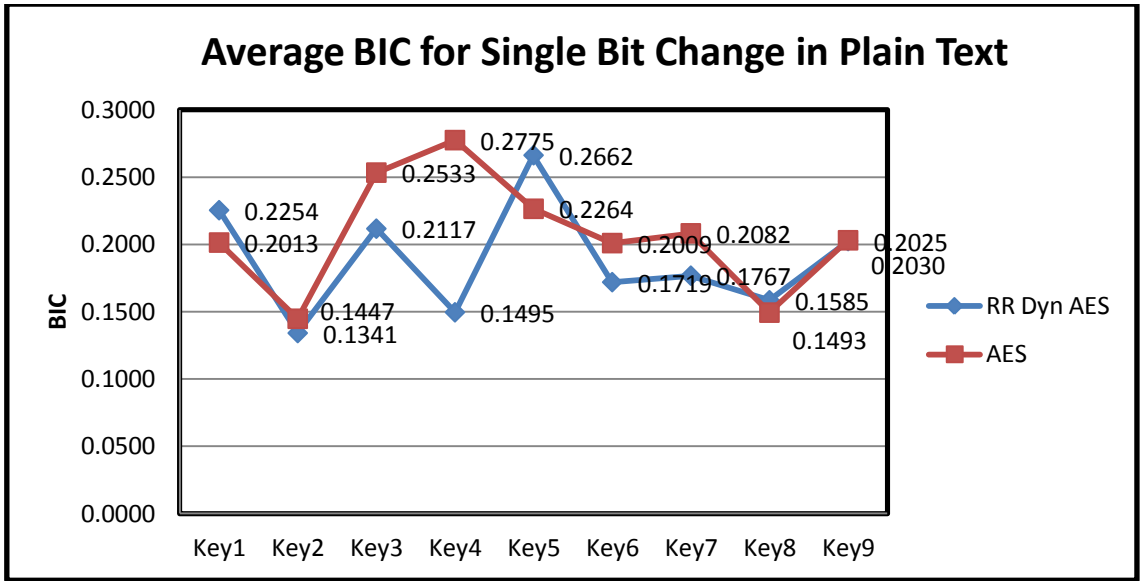

Fig 10: Graphical representation of Average BIC of RR Dynamic AES and Standard AES with one bit change in Plain Text

7. CONCLUSION

In this article the performance of standard AES and RR Dynamic AES analyzed for the criterion like strict avalanche criterion and bit independence criterion. Both standard AES and RR Dynamic AES are shown to meet all of the criteria. However, both the strict avalanche criterion and the bit independence criterion yielded better results for RR Dynamic AES. As a result, the new algorithm with eight rounds of encryption with dynamic S-Boxes yields better results and is more resistant to algebraic attacks. In future work RR Dynamic AES will be tested for its efficiency in encryption of different format of data like text documents, images and sound files and compared against standard AES.

8. REFERENCES

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

[2] Krishnamurthy G N. and Ramaswamy V. 2008. Making AES Stronger: AES with Key Dependent S-Box, International Journal of Computer Science and Network Security, 9(8).

[3] Piotr M. 2009, Generating Pseudorandom S-Boxes a Method of Improving the Security of Cryptosystems Based on Block Ciphers, Journal of Telecommunications and Information Technology.

[4] ElGhafar A., Rohiem A., Diaa A., Mohammed F. 2009, Generation of AES Key Dependent S-Boxes using RC4 Algorithm, 13th International Conference on Aerospace Sciences & Aviation Technology, ASAT- 13, May pp. 26-28.

[5] Ghada Z., Abdennaceur K., Fabrice P. and Daniele F. 2009, On Dynamic chaotic S-BOX, IEEE

[6] Cui J., Huang L., Zhong H., Chang C. and Yang W 2011. An Improved AES S-Box and Its Performance Analysis, International Journal of Innovative Computing, Information and Control.

[7] Julia Juremi Ramlan Mahmod Salasiah Sulaiman Jazrin Ramli 2012, Enhancing Advanced Encryption Standard S-Box Generation Based on Round Key, International Journal of Cyber-Security and Digital Forensics (IJCSDF) vol. 1, no. 3, pp. 183-188.

[8] Dara M. and Manochehri K. 2013, A Novel Method for Designing S-Boxes Based on Chaotic Logistic Maps Using Cipher Key, World Applied Sciences Journal vol. 28, no. 12, pp. 2003-2009.

[9] Mohammed Mahmoud E., Abd El Hafez A., Talaat A. and Zekry A 2013. Dynamic AES-128 with key-dependent s-box, International Journal of Engineering Research and Applications, vol. 3, no. 1, pp. 1662-1670.

[10] Ahmed F. and Elkamchouchi D. 2013, Strongest AES with S-Boxes Bank and Dynamic Key MDS Matrix (SDKAES), International Journal of Computer and Communication Engineering.

[11] Adi Narayana Reddy K. and Vishnuvardhan B. 2014, Secure Linear Transformation Based Cryptosystem using Dynamic Byte Substitution, International Journal of Security, vol. 3, no. 8.

[12] Kazys K., Gytis V., Robertas S. 2015, An Algorithm for Key-Dependent S-Box Generation in Block Cipher System, INFORMATICA, vol. 26, no. 1, pp. 51-65.

[13] Balajee Maram K., Gnanasekar J. M. 2016, Evaluation of Key Dependent S-Box Based Data Security Algorithm using Hamming Distance and Balanced Output, TEM Journal, vol. 5, no. 1.

[14] Daemen J., Knudsen L. and Rijmen V 1997., The block Cipher Square. Fast Software Encryption 97, Springer-Verlag, pp. 149-165.

[15] Daemen J. and Rijmen V., AES Proposal: Rijndael, second Version, AES submission.

[16] Lucks S. 2000, Attacking Seven Rounds of Rijndeal under 192-bit and 256-bit keys, The third Advanced Encryption Standard Candidate Conference, NIST, pp. 215-29.

[17] Ferguson N., Kelsey J., Lucks S., Schneier B., Stay M., Wagner D. and Whiting D. 2001, Improved

Cryptanalysis of Rijndeal, Fast Software Encryption 2000, Lecture notes in Computer Science, Springer-Verlag, vol. 1978, pp. 213-230.

[18] Webster A.F. and Travares S.E. 1998, On The Design of S-boxes, Queen's university Kingston, Springer-verlag ,Canada.

[19] Webster A.F. and Tavares S.E. 1986, On the Design of S-Boxes, Advances in Cryptology, Proceedings of CRYPTO 85, Springer Verlag, New York , pp. 523-534.

[20] Agarwal P., Singh A.,Kilicman A. 2018, Development of Key Dependent Dynamic S-Boxes with Dynamic Irreducible Polynomial and Affine Constant, Advances in Mechanical Engineering.