International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

A Novel Approach to Building Substitution-Boxes with Dihedral Group

Shamim[a], Nasir Siddiqui[b]

[a] *Department of Mathematical Sciences, University of Engineering and Technology Taxila, Pakistan*

[b] *Department of Mathematical Sciences, University of Engineering and Technology Taxila, Pakistan*

A B S T R A C T

S-boxes play a pivotal role in modern encryption algorithms, their cryptographic properties are paramount and crucial to guaranteeing the safety of sensitive information. This research paper explores a novel approach to building of 8x8 S-boxes using Dihedral Group. For this purpose, we draw the Cayley Graph of Dihedral Group and create an adjacency matrix of Dihedral Group. Next, an adjacency matrix is used to the Galios field GF(2^(8)) elements and apply affine transformations to create S-boxes. The resulting S-boxes are evaluated for their cryptographic properties, such as non-linearity, differential uniformity, and algebraic complexity.

Keywords: Dihedral Group, Adjacency Matrix, Cayley Graph, S-Box, Image Encryption.

1. INTRODUCTION

The study and application of secure communication methods when facing adversaries or third parties is known as cryptography. In general, cryptography is the study and creation of protocols that shield confidential communications from public access or third parties. [1]. Cryptography is used to protect information by transforming it into a form that is unable to be read or understood by individuals not authorized [2]. This is done by using a mathematical algorithm to encrypt the information, which scrambles it so that it is no longer readable. The encrypted information is then called ciphertext. The recipient of the encrypted information can decrypt it using the same algorithm and a secret key [3]. The two primary categories of cryptology are symmetric and asymmetric cryptography. Apply the same keys for both encryption and decryption in symmetric cryptography [4]. This type of cryptography is typically used for applications where speed is important, such as secure communication over a network. Two separate keys are used in asymmetric cryptography: one for encryption and another for decryption. The kind of cryptography generally employed for applications where security is more crucial than speed, such as digital signatures [5]. Here are some examples of cryptography, The Caesar cipher is a simple symmetric cipher that replaces each letter in a message with the letter that is three places after it in the alphabet. For example, the message "hello" would be encrypted as "kdliw". Data encryption is frequently done using the symmetric recognized cipher while the Advanced Encryption Standard (AES). AES is considered to be very secure and is used in many applications, such as secure communication over the internet and encryption of hard drives [6]. The RSA algorithm is an asymmetric cipher that is used for digital signatures and other applications where security is important. RSA is considered to be very secure and is used in many applications, such as secure email and online banking. Substitution boxes are fundamental components in modern cryptographic systems, used to introduce nonlinearity and confusion to encryption algorithms. S-boxes map input bit sequences to output bit sequences, thereby introducing complexity and enhancing the security of cryptographic operations [7]. The design and construction of secure and efficient S-boxes have been subjects of extensive research within the domain of cryptography [7, 8]. The advancement of robust and safe cryptographic algorithms is crucial in the face of increasing threats to data security [9, 10]. The layout of S-boxes with desirable properties of cryptography is an important aspects of this endeavor.

S-box Proposed Method

There are four essential steps in the suggested process for building S-boxes. First, we create Cayley diagram using the Dihedral Group elements. Next**,** form the Cayley graph adjacency matrix of the dihedral group. Finally, use the adjacency matrix to perform affine transformation on the elements of the Galois field.

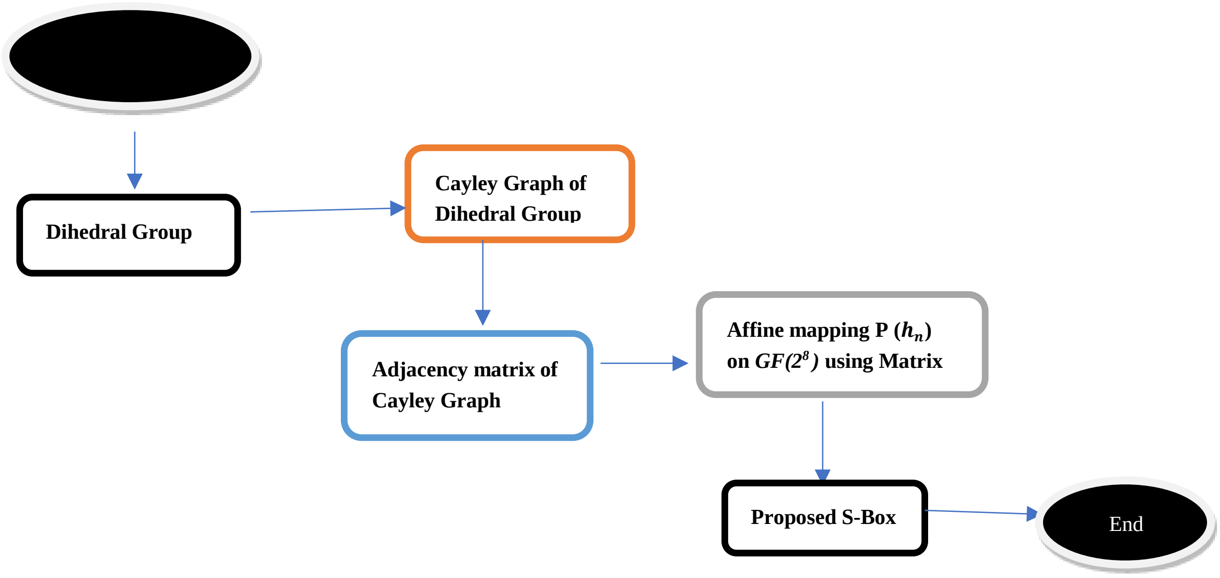

Fig 1. Algorithm for proposed S-Box

2.1 Dihedral Group

A dihedral group is a collection of regular polygonal symmetries, which includes reflections and rotations. The Dihedral group is composed of the related rotations and reflections. Finite representation of Dihedral Group is $D_8 =< a, b = a^4 = b^2 = (ab)^2 = 1 >$ and elements of Dihedral Groups are $1, a, a^2, a^3, ab, a^2b, a^3b$

2.2 Cayley Graph of Dihedral Group

Now, we draw the Cayley graph by using elements of Dihedral Group. Cayley graph are a natural way to represents groups as graphs. Cayley graph is graph that is associated to a group and set of generators for that group. The vertices of the groups are the elements of the groups, and there is an edge between two vertices iff they differ by one the generators. The Cayley graph of Dihedral is show in fig 2.

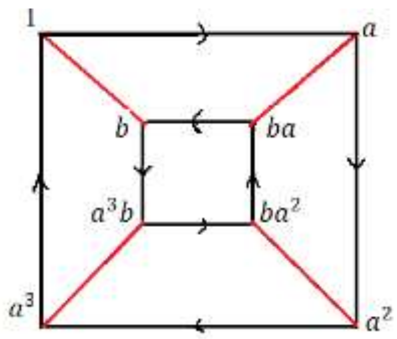

Fig 2. Cayley Graph of Dihedral Group

2.3. Adjacency matrix of Cayley graph

In this step, we generate an adjacency matrix from the Cayley graph of Dihedral Group. Adjacency matrix, sometimes called the connection matrix. If two variables, Vi and Vj, are labeled with numbers 0 and 1, respectively, and the condition is whether or not they are adjacent, the matrix is called an adjacency matrix. It is composed of rows and columns. In the case of a directed graph, the value of A[Vi][Vj] = 1 if an edge exists connecting vertices i, Vi, and j, Vj. If not, the value = 0 [11]. The Cayley graph from Fig. 2 has an adjacency matrix, which is shown below.

$$A=\begin{bmatrix}0&1&0&0&1&0&0&0\\0&0&1&0&0&0&0&1\\0&0&0&1&0&0&1&0\\1&0&0&0&0&1&0&0\\1&0&0&0&0&1&0&0\\0&0&0&1&0&0&1&0\\0&0&1&0&0&0&0&1\\0&1&0&0&1&0&0&0\end{bmatrix}$$

2.4 Affine mapping on a Galois field with an adjacency matrix

Upon utilizing the acquired adjacency matrix A on $GF\,(2^8)$ the outcome revealed no uniqueness. While elements of S-box must indicate uniqueness and for this reason we propose a set of transformation P

$$P(h_n) = Ah_n + h_{n+i\,(mod256)} \qquad (1)$$

In equation (1), h_n represents the elements of Galois field on $GF\,(2^8)$, where n=0,1,2,3……..255. We checked all the values from 0 to 255 in i using (1) and obtained different S-box for *i*= 1,2,4,8,16,32,64,128. We choose *i*=8 for construction process of suggested S-box 1 shown in table 1. The suggested S-Box 1 is given in table 2. Similarly for i =2 the suggested S-box 2 is given in table 3.

Table 1- Shows the proposed S-Box 1 construction for i = 8.

$GF(2^8)$	$P(h_n) = Ah_n + h_{n+i\,(mod256)}$	**Proposed S-Box**
0	$P(h_0) = Ah_0 + h_{0+8\,(mod256)}$	0
1	$P(h_1) = Ah_1 + h_{1+8\,(mod256)}$	222
2	$P(h_2) = Ah_2 + h_{2+8\,(mod256)}$	29
.	.	.
.	.	.
.	.	.
254	$P(h_{254}) = Ah_{254} + h_{254+8(mod256)}$	23
255	$P(h_{255}) = Ah_{255} + h_{255+8(mod256)}$	252

Table 2 -Proposed S-Box 1 for i =8

0	**222**	**29**	**189**	**166**	**65**	**184**	**153**	**156**	**242**	**110**	**64**	**243**	**234**	**141**	**40**
223	73	192	152	214	168	129	103	12	96	174	5	187	202	66	63
80	237	123	159	254	77	255	134	155	105	102	93	200	90	35	48
59	135	31	46	106	211	32	251	167	160	228	162	213	203	18	115
185	205	241	126	57	169	130	197	210	113	30	104	2	92	170	224
143	109	218	50	107	13	72	208	193	54	118	53	42	122	172	204
151	78	145	163	85	244	220	27	227	116	217	239	191	183	195	38
125	249	69	97	45	68	173	114	87	219	230	117	138	21	52	154
165	120	95	19	124	9	185	75	47	121	33	3	112	137	60	238
140	43	41	247	62	61	15	245	253	226	132	196	100	28	207	81
232	240	119	36	149	194	225	44	37	147	67	133	216	157	79	39
179	17	250	231	139	164	190	175	158	25	146	14	84	11	142	128
70	182	86	171	20	212	91	6	221	88	49	24	22	26	58	215
94	51	235	8	209	82	181	180	148	161	144	1	10	101	55	4
199	176	131	71	16	89	99	248	111	74	229	206	233	236	201	178
150	76	83	188	136	56	98	246	198	7	108	34	177	127	23	252

Table 3- Proposed S-Box 2 for i =2

0	**222**	**29**	**189**	**166**	**65**	**184**	**153**	**38**	**195**	**183**	**191**	**239**	**217**	**116**	**227**
223	73	192	152	214	168	129	103	154	52	21	138	117	230	219	87
80	237	123	159	254	77	255	134	224	170	92	2	104	30	113	210
59	135	31	46	106	211	32	251	204	172	122	42	53	118	54	193
185	205	241	126	57	169	130	197	48	35	90	200	93	102	105	155
143	109	218	50	107	13	72	208	115	18	203	213	162	228	160	167
151	78	145	163	85	244	220	27	40	141	234	243	64	110	242	156
125	249	69	97	45	68	173	114	63	66	202	187	5	174	96	12
165	120	95	19	124	9	186	75	178	201	236	233	206	229	74	111
140	43	41	247	62	61	15	245	252	23	127	177	34	108	7	198
232	240	119	36	149	194	225	44	215	58	26	22	24	49	88	221
179	17	250	231	139	164	190	175	4	55	101	10	1	144	161	148
70	182	186	171	20	212	91	6	39	79	157	216	133	67	147	37
94	51	235	8	209	82	181	180	128	142	11	84	14	146	25	158
199	176	131	71	16	89	99	248	238	60	137	112	3	33	121	47
150	76	83	188	136	56	98	246	81	207	28	100	196	132	226	253

3. Algebraic analyses and comparisons

Several tests, including non-linearity, the linear approximation probability (LP), the strict avalanche criterion, the bit independence criterion (BIC), and the differential approximation probability (DP) are included in algebraic analyses. We verified our proposed S-boxes algebraic analyses. Additionally, we compare and contrast our S-box with other S-boxes that already exist.

3.1. Non- linearity

A Boolean expression Nonlinearity could, as mentioned, become the division of the function from the set of all affine functions. Another definition of non-linearity is the number of bytes that should be converted into the Boolean function truth table to obtain adjacent affine function. We can formulate a mathematical relationship between the Walsh-Hadamard transformation and non-linear nature of the n-variable Boolean function

$$\boldsymbol{N(f) = 2^{n-1} - 2^{\frac{n}{2}-1}} \qquad \textbf{(2)}$$

The mean non-linearity of our recommended S-boxes is 112, with a maximum and minimum of 112.

Table 4 – Non-linearity Comparison

S-Boxes	Min	Max	Avg
Proposed S-Box 1	112	112	112
Proposed S-Box 2	112	112	112
Xyi	104	106	105
Gray	112	112	112
APA	112	112	112
Prime	95	104	99.5
AES	112	112	112
Skipjack	104	108	105.75

3.2. Strict avalanche criterion

The SAC relies on modifications to the output bits and input results. When an input changes by just one bit. S-box satisfies SAC, and half of the output bits are left. Table 5 lists the differences between the suggested S-boxes and the S-Boxes that are now in use.

$$\frac{1}{2}\sum_{i=1}^{n} |f(x) \oplus f(x \oplus e_i) = 2^{n-1} \qquad (3)$$

Table 5 – SAC Comparison

S-Boxes	Max	Min	Avg	Square deviation
Proposed S-Box 1	0.5625	0.4375	0.5043	0.0309
Proposed S-Box 2	0.5625	0.4531	0.5075	0.0285
AES	0.562	0.453	0.504	0.0156
Gray	0.562	0.437	0.499	0.015
Skipjack	0.593	0.39	0.503	0.024
APA	0.562	0.437	0.5	0.016
Prime	0.671	0.343	0.516	0.032
Xyi	0.609	0.406	0.502	0.022

3.3. Probability of linear approximations

An events maximum output imbalance value is examined using the linear probability method. Linear probability can be calculated using the formula in (4).

$$LP = max_{u_x,u_y}|\#x \in {}^{A}/_{X} \; .u_x = S(x).u_y/2^n - {}^{1}/_{2}| \qquad (4)$$

The input differentials are represented by the variable u_x , the output differentials are represented u_y. Table 6 presents the outcome of comparing several S-boxes for LAP.

Table 6 – LAP Comparison

S-Boxes	Max Value	Max LP
Proposed S-Box 1	144	0.0621
Proposed S-Box 2	144	0.0621
AES	144	0.062
Prime	162	0.132
Xyi	168	0.156
Gray	144	0.062
Skipjack	156	0.109
APA	144	0.062

3.4. Differential approximation probability

As this criteria is applied to measure the differential homogeneity of the S-boxes. When just one input bit is changed in this manner, a specific output adjustment is required. The XOR distribution of the substitution boxes inputs and outputs determined.

$$DP = [\#\{x \in X | S(x) \oplus S(x \oplus \nabla_x) = \nabla_y\}/2^m] \qquad (5)$$

Where the differential input is denoted by $\nabla_x$and the output differential by ∇_y.

Table 7 – DP Comparison

S-Boxes	Proposed S-Box 1	Proposed S-Box 2	Gray	Prime	APA	Xyi	Skipjack	AES
Max DP	**0.015**	**0.015**	**0.0156**	**0.281**	**0.015**	**0.0468**	**0.0468**	**0.015**

3.5. Criteria for Bit Independence

A notable criterion proposed by Webster and Tavares states that in a cryptosystem, when one input bit changes, two output bits must likewise change. As a result, it becomes difficult to alter the system without affecting its single bit.

Table 8 – BIT Comparison

S-Boxes	Avg	Square Deviation	Min
Proposed S-Box 1	112	0	112
Proposed S-Box 2	112	0	112
Gray	112	0	112
Prime	101.71	3.53	94
Skipjack	104.14	1.767	102
Xyi	103.78	2.743	98
APA	112	0	112
AES	112	0	112

4. Image Encryption

Majority logic criteria (MLC) form the basis of the statistical analysis of image encryption applications. Its goal is to distort the image, and such distortion stands for the applications legitimacy. Entropy, contrast, correlation, energy, and a homogeneity test are all included in this analysis. The encryption process is carried out on Lena and Baboon images. Figures 3 and 4 depict the images encryption. The real image is depicted in Figures 3 (a) and 4 (a). Figures 3 (b) and (c) depict the encrypted images for S-boxes 1 and 2. Figures 4(b) and (c) depict the images that are encrypted for S-boxes 1 and 2.

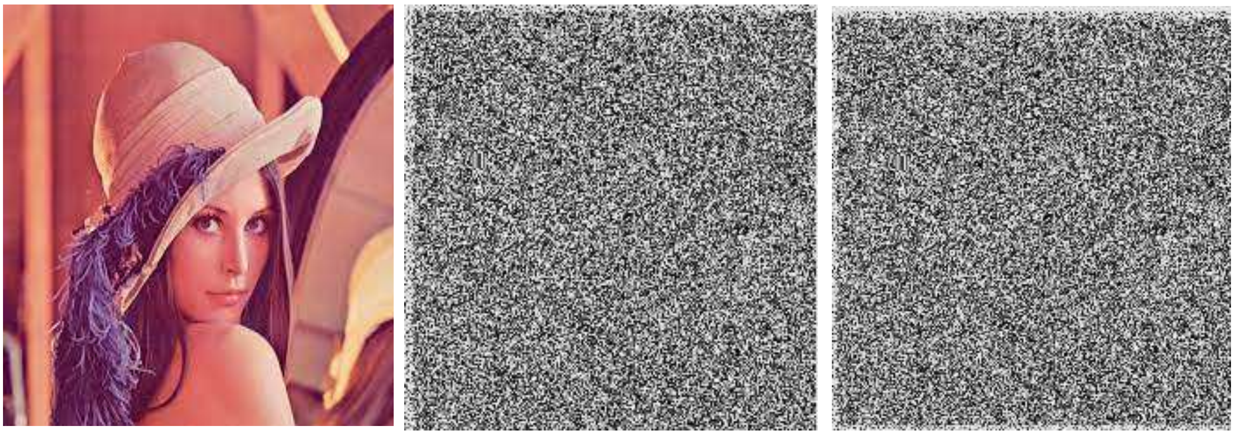

Fig. 3 (a) (b) (c)

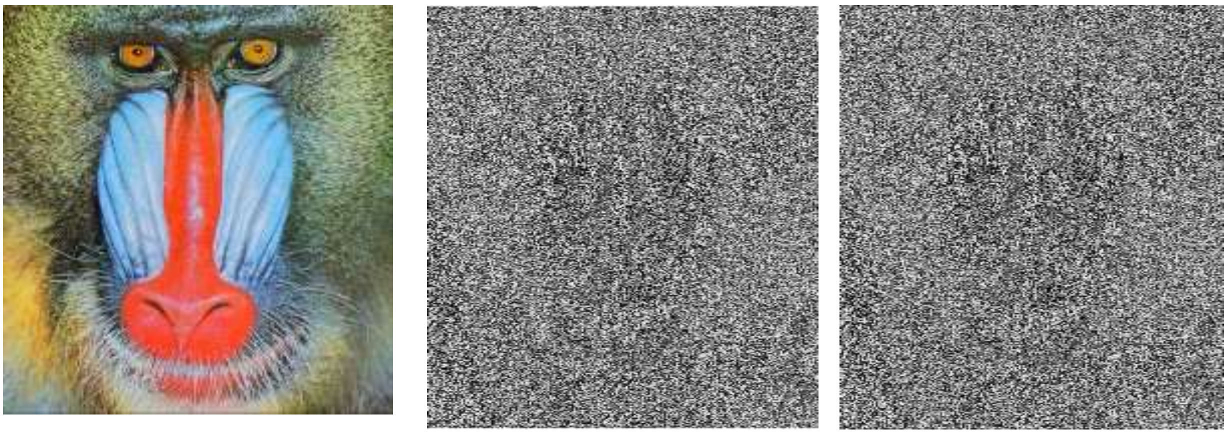

Fig. 4 (a) (b) (c)

5. Conclusions

Utilizing in this research a novel approach to build 8x8 S-boxes with the Dihedral Group. We create its adjacency matrix and draw the Cayley Graph of the Dihedral Group for this purpose. The adjacency matrix is then applied to the Galios field $GF(2^8)$ elements using a different transformation to generate S-boxes. We verify the cryptology robustness of the S-boxes being suggested by analyzing their algebra-based robustness through standard S-Box tests. Additionally, the suggested S-boxes for encrypting images and running arithmetical tests to assess their effectiveness. These studies show that the suggested S-box layout is effective for apps for image encryption. Later, the proposed method can be extended to construct n x n S-boxes with various action groups and n x n adjacency matrices.

References

[1] J. Menezes, P.C. Oorschot and S. A Vanstone. “Handbook of Applied Cryptography.” CRC, 2001.

[2] Damico, Tony M. “A Brief History of Cryptography.” Inquiries Journal. 1 Nov.2009, www.inquiriesjournal.com/articles/1698 /a- Brief -history-of-Cryptography.

[3] R. A. Mollin, “An Introduction to Cryptograph.” Chapman and Hall/ CRC, 2007

[4] N. Siddiqui, H. Khalid, F. Murtaza, M. Ehatisham-ul-Haq and M. A. Azam. “A Novel Algebraic Technique for Design of Computational Substitution-Boxes Using Action of Matrices on Galois Field.” IEEE Access, vol.8, 2020, pp.197630-197643., doi10.1109/ACCESS.2020.3034832

[5] A. Razaq et al., A Novel Method for Generation of Strong Substitution Boxes Based on Coset Graphs and Symmetric Groups. in IEEE Access, vol. 8, pp. 75473-75490, 2020.

[6] A. Razaq, A. Yousaf, U. Shuaib, N. Siddiqui, A. Ullah and A. Waheed. “A Novel Construction of Substitution Box Involving Coset Diagram and a Bijective Map.” Security and Communication Networks, vol. 2017, pp. 1-16., doi: 10.1155/2017/5101934

[7] A. Anees and Yi-Ping. P. Chen. “Designing secure substitution boxes based on permutation of Symmetric group.” Neural Computing and Applications, vol. 32, no. 11, 2019, pp. 7045-7056., doi: 10.1007/s00521-019-04207-8.

[8] T. Shah and A. Qureshi. “S-Box on Subgroup of Galois Field.” Cryptography, vol. 3, no. 2, 2019, doi: 10.3390/cryptography3020013.

[9] N. Siddiqui, F. Yousaf, F. Murtaza, M. Ehatisham-ul-Haq, M. U. Ashraf, A. M. Alghamdi and A. S. Alfakeeh. “A Highly Nonlinear Substitution-Box (S-Box) Design using action of Modular Group on a Projective Line over a Finite Field.” Plos one, vol. 15, no. 11, 2020, doi: 10.1371/journal.pone.0241890.

[10] I. Shahzad, Q. Mushtaq and A. Razaq. “Construction of New S Box using Action of Quotient of the Modular Group for Multimedia Security.” Security and Communication Network, vol.2019, 2019, pp.1-13.

[11] Adam Drozdek. Data Structures and Algorithms in C++-2 nd ed. Brooks/Cole, 2001.

[12] H. Delfs and H. Knebl. Introduction to cryptography: principles and applications. Springer, 2002

[13] N. Siddiqui, U. Afsar. “A Novel Construction of S16 AES S-boxes.” International Journal of Computer Science and Information Security (IJCSIS), Vol. 14, No. 8, August 2016.

[14] Daemen, Joan and Vincent Rijmen. “The Block Cipher Rijndael.” Smart Card Research and Advanced Application Conference (1998).

[15] Nizam Chew LC, Ismail ES. S-box Construction Based on Linear Fractional Transformation and Permutation Function. Symmetry. 2020; 12(5):826.

[16] A. Altaleb, M. S. Saeed, I. Hussain, M. Aslam. ”An algorithm for the construction of substitution box for block ciphers based on projective general Linear group.” AIP Advances 1 March 2017; 7 (3): 035116.

[17] N. Siddiqui, U. Afsar. “A Novel Construction of S16 AES S-boxes.” International Journal of Computer Science and Information Security (IJCSIS), Vol. 14, No. 8, August 2016.

[18] Razaq, A., Ahmad, M., Yousaf, A. et al. A Group Theoretic Construction of Large Number of AES-Like Substitution-Boxes. Wireless Pers Commun 122, 2057–2080 (2022).

[19] T. Shah, I. Hussain, M. Gondal and Y. Wang. . Analyses of SKIPJACK S-box. World Applied Sciences Journal. (2011). 13. 2385-2388.

[20] B. Arshad, N. Siddiqui, Z. Hussain. ”A Novel Method for Designing Substitution Boxes Based on Mobius Group.” 15 March 2021,