VFAST Transactions on Mathematics
http://vfast.org/journals/index.php/VTM@ 2021, ISSN(e): 2309-0022, ISSN(p): 2411-6343
Volume 10, Number 1, January -June, 2022 *pp: 14-31*

Algebra Based Encryption and Decryption Algorithms

Shakeel Ahmed Kamboh[1*], **Suhail Aslam Khaskheli**[2], **Abbas Ali Ghoto**[1], **Sunny Kumar Aasoori**[1], **Muzaffar Bashir Arain**[1]

[1*]Department of Mathematics and Statistics, QUEST, Nawabshah ; [2]Department of General Faculty, Faculty of Science and Technology, Shaheed Benazir Bhutto University, Nawabshah, SBA.

Keywords: *Encryption and Decryption Algorithm, Blok Ciphers, DES Algorithm, Applied Cryptography, Network Security.* ***Subject Classification***: *Applies Mathematics, Coding Theory, Computational Science .*

Journal Info:
Submitted:
April 10, 2022
Accepted:
May 16, 2022
Published:
June 30, 2022

Abstract In this study an encryption/decryption algorithm is proposed and developed. The developed algorithm is based on the idea that any given plain text can be encrypted like a block cipher with a combination of three encryption keys k_1, k_2, k_3 that use any value between $N = 1, 2, 3, n, .$ Then the cipher values can be used to make the blocks of alphabets containing only A, B, C, D, E, F, G, H, I, J, each block is separated by a space. The steps of algorithm could also be reversible for decryption of the cipher text. A MATLAB code is written to implement the algorithm and tested different input messages.Secret message consists of website link and bank account details. The specialty of the algorithm is that it can be flexibly used to encrypt and decrypt the secret messages containing not only English alphabets but also those messages containing the numbers, punctuations, elementary mathematics operations and the special characters. The performance of the algorithm is evaluated in terms of computational time, memory usage. From the analysis it is found that the proposed algorithm is faster in terms of execution time as compared to the modern algorithm which makes the algorithm computationally secure. The proposed research particularly contributes as the addition of knowledge in the field of cryptography and generally to the information security; consequently can be beneficial to the society.

***Correspondence Author Email Address:**
shakeel.maths@yahoo.com

1 Introduction

Cryptography is concerned with the encryption and decryption of secret messages and perhaps is an ancient art of coding private information. More generally, cryptography is concerning construct and analyzing the algorithms that avoid third party or the public as of interpretation confidential communication [1]. The history of cryptography dates bakes to around 1900 B.C. when an Egyptian inscription carved used substandard hieroglyphs to transform the original message [2]. The different forms of cryptography have been appeared independently in various civilizations. The classical applications of cryptography rang from diplomatic missive to time of war combat strategy. After the computer era and extensive advance of computer communications the cryptography has become an indispensable tool for secure communications over the network. There are several ways of classifying cryptographic algorithms but mainly are classified into two categories i.e., Secrete key cryptography (also called symmetric encryption) and public key cryptography (also called asymmetric encryption). In addition to these two types of encryption methods; Hash Functions are also used that apply mathematical transformation to irreversibly "encrypt" information, providing a digital fingerprint and mainly concerned with message integrity. The Symmetric encryption uses a single key for both encryption and decryption and is primarily used for privacy and confidentiality. The idea of symmetric key encryption is illustrated by Fig 1. Where a plain text is encrypted by a secret key and the resulted ciphertext is send to receiver. Then the receiver use similar secret key to decrypt the received message and recovers the original message. Asymmetric encryption uses one key for encryption and another for decryption mostly applied for verification, non-repudiation, and key swap the idea of asymmetric key encryption is illustrated by Fig 2. Where a plain text is encrypted by a public key and the resulted cipher text is sent to receiver [3-4]. Then the receiver uses different key (private key) to decrypt the received message and recovers the original plain text.

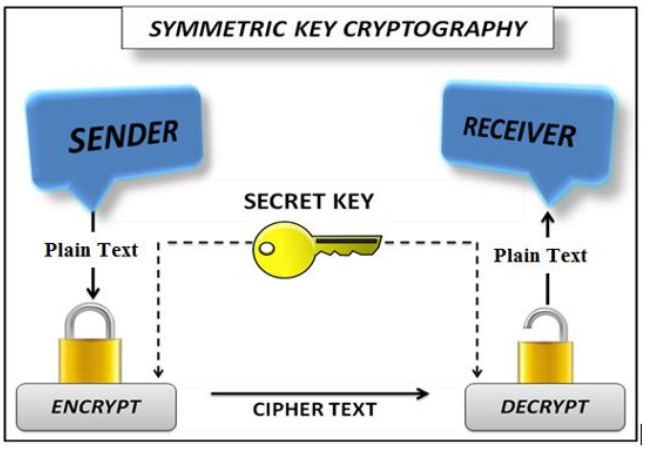

Figure 1. Illustration of Symmetric key encryption

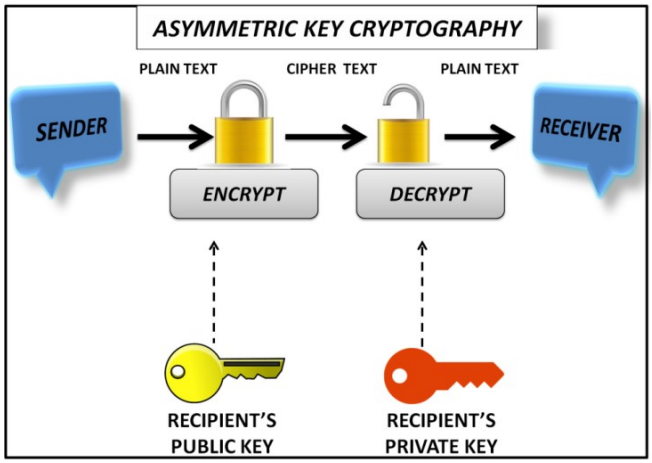

Figure 2. Illustration of Asymmetric key encryption

2 BASIC TERMINOLOGY

In order to understand the principles and algorithms of cryptography it is worthwhile to understand the basic terms. This section will define the most basic terms that will be required to understand the algorithms of cryptography.

Plaintext: The original secret text message that is intended to send to another person or party is called a plaintext. For example, Alice is a person who needs to send out the communication Hello, Who are you? to his friend Bob. Here the message Hello, Who are you? is called plaintext [5-6]. The plaintext may contain alphabets of any language, numbers, punctuations, special characters, etc.

Ciphertext: The message that is transformed into unreadable or encoded form and obtained by applying any encryption method is called a ciphertext. An example Thoor, Tre hud xos@ is a ciphertext of the plaintext communication Hello,Who are you [7-8]. Cipher: Cipher is used to transforms plaintext to cipher-text, this process is called encryption. In further: it is a mechanism of convert clear and understandable information into meaningless information [9-10]. The cipher is based on some mathematical operations independent of the plaintext. Different operations along with secret values will yield different ciphertext.

Keys: A key is a numeric or alpha numeric manuscript might be a special character and is considered as a main secret value in any encryption/decryption algorithm. The key is use on the moment of encryption take position on the plaintext and on the moment of decryption takes place on the ciphertext. The choice of key in cryptography is very essential since the protection of encryption algorithm depends directly on the choice of more secret key. For example Alice used a key of k=3 to encrypt the plaintext President then ciphertext produced will be Suhvlghqw [11 12].

Encryption: A systematic procedure of converting the given information (plaintext) into the encoded information (ciphertext) is called as encryption. Cryptography uses the encryption techniques to send secret message(s) securely so that only the intended person may read the sent message(s). Mainly, the procedure of encryption requires two things an encryption algorithm and a key, usually the encryption takes place at the sender side [13, 14].

Decryption: The decryption is the reverse procedure of the encryption that is; in decryption the original information (plaintext) is recovered from the hidden or coded information (ciphertext). Usually, the

decryption takes place at the receiver side as the receiver already may have the method or algorithm and decryption key [15-16]. If the decryption process is applied by a third party between sender and receiver then it will be considered as a cryptanalytic attack.

3 BREIF REVIEW OF THE PERFORMANCE OF DIFFERENT SYMMETRIC KEY ALGORITHMS

The modern symmetric key methods are based on the concept of bit key and binary blocks with logical operations. Each method has its own merits and demerits depending upon the level of security and computational complexity. In this section, the performance of different cryptographic algorithm is reviewed. In this context, a relative study on DES, 3DES, AES was done by [17] using Java programming on the basis of the parameter rounds, block size, key size, encryption/decryption time, CPU process time in the form of throughput and power utilization. He concluded that the AES has benefit more than the additional 3DES and DES in conditions of throughput (Throughput = Plain Text (MB) / Encryption or decryption time (sec)) and decryption time. Another experimental analysis of AES, DES and RSA (a public key encryption algorithm) is conducted [18] and it was accomplished that AES algorithm consume smallest amount encryption time and RSA use highest encryption time. They also observed that decryption of AES algorithm is improved than other algorithms. [19] Analyzed encryption time for different symmetric key algorithms for a variety of file features like different information type, information compactness, information volume and key range. From the simulated results it is concluded that the encryption time and data size is proportional to each other. As the size of information increase the encryption time also increase proportional to information size and vice versa. For all block cipher algorithms AES appear to be fastest block cipher with throughput or encryption speed of 108MB/sec. Recently, a latest time assessment model base on random number generating mechanism is projected by [20] to analyze the time-consuming of the known block cipher symmetric cryptographic algorithms. Their theoretical results showed that under the similar key length and for the same size of the processed data, Triple-DES is about quite a few hundred times slower than AES, DES and IDEA. In order to know whether to choose AES, RSA or IDEA a comparative study was carried out by [21] by considering the factors such as the key length, cipher kind, block size, protection, likelihood key, probable ACSII printable character keys, time necessary to ensure all probable keys. They proved that the AES is better than IDEA and RSA. Similarly, another performance comparison between the DES, 3DES, AES and Blowfish was implemented and simulated on .NET environment by [22]. Their conclusion reveals that 3DES has a better performance result with ECB (Electronic Codebook) mode and CBC (Cipher Block Chaining) mode than other common encryption algorithms used. [23] Presented the implementation limitations of DES, 3DES, CAST-128, BLOWFISH, IDEA, AES, and RC6 symmetric techniques and RSA of asymmetric techniques. The analysis of the results showed that asymmetric algorithms are better in security; however they take more time for processing and require more memory. [24-25] Demonstrated that the AES algorithm is limited just for text as an input. So it is challenging to execute the AES algorithm for a variety of type of effort and requires less decryption time; it also has the more time complexity. From the above review it can be concluded that the major disadvantage of symmetric key encryption algorithms is the sharing of the same key. In classical methods the number of keys is limited consequently the brute force or cryptanalysis

attack may easily break the encrypted message. While among the modern methods the AES is reported more secure and fast as compared to other methods. But firstly, AES is complicated to implement and secondly the encrypted message has block of (4+4) bits (meaning a pair of characters) that may have side channel attack. Therefore, the proposed study is the motivation for the development of a simple but computationally secure symmetric encryption/decryption algorithm.

4 PROPOSED METHODOLOGY

The formulation of symmetric encryption models involves various steps including different aspects of symmetric encryption key. For the sack of brevity the major steps involved in the research methodology are listed below:

Step 1E. Define the secret messages (SM) to be encrypted/decrypted. In general, any message having sensitive or intelligence information can be used. But in this study the following secrete message will be used for testing and implementation purpose.

Secret message-(SM): Open the bank website http://www.banknp.com the user name is BC2016 and the password is my20161516banknp transfer 1 million US-dollar to this account111562938-5.

Step 2E. Assign and label the nonnegative integer values to the alphabets, digits, operators, brackets and special characters. Total 97 symbols are used that will be sufficient for the conversion of given plaintexts to ciphertexts. The list of such symbols and their assigned values is given in the following Table 1.

A	B	C	D	E	F	G	H	I	J
1	2	3	4	5	6	7	8	9	10
K	L	M	N	O	P	Q	R	S	T
11	12	13	14	15	16	17	18	19	20
U	V	W	X	Y	Z	a	b	c	d
21	22	23	24	25	26	27	28	29	30
e	F	g	H	i	j	k	l	m	n
31	32	33	34	35	36	37	38	39	40
o	P	q	R	s	t	u	v	w	x
41	42	43	44	45	46	47	48	49	50
y	Z	0	1	2	3	4	5	6	7
51	52	53	54	55	56	57	58	59	60
8	9	!	@	#	$	%	&	^	*
61	62	63	64	65	66	67	68	69	70
_	=	+	-	×	÷	?	>	<	~
71	72	73	74	75	76	77	78	79	80
;	:	“	”	,	`	.	\	/	{
81	82	83	84	85	86	87	88	89	90
}	(	)	[	]	|	©			
91	92	93	94	95	96	97			

Table 1. List of plaintext symbols and their values

Step 3E. Select the proper keys k_1, k_2, k_3 from $N = 1, 2, 3 \ldots n$ to encrypt the given plaintext and apply the following three operations:

$$S_1 = pv.k_1, \tag{1}$$

$$S_2 = S_1 + k_2, \tag{2}$$

$$S_3 = S_2 - k_3 = cv. \tag{3}$$

where pv represents the plain values and $k_2 \geq k_3$ to for non-negative values. The idea behind using these operations is that the plaintext is converted easily to cipher values without using any other operations like modular arithmetic, matrices or logical operations. Since, the multiplication, addition and subtraction are the most basic arithmetic operations. The division is not used because it will produce the cipher values into fractions and will mislead to identify the character values. As for each character or symbol only a whole number can be used to label.

Step 4E. In the final step, S_3 produces the streams of cipher values containing the digits {0, 1, 2, 3, 4, 5, 6, 7, 8, 9}. Each individual stream of can be converted into the blocks of alphabets containing only $A, B, C, D, E, F, G, H, I, J$. The framework of the proposed encryption algorithm is exhibited by the following Figure 3.

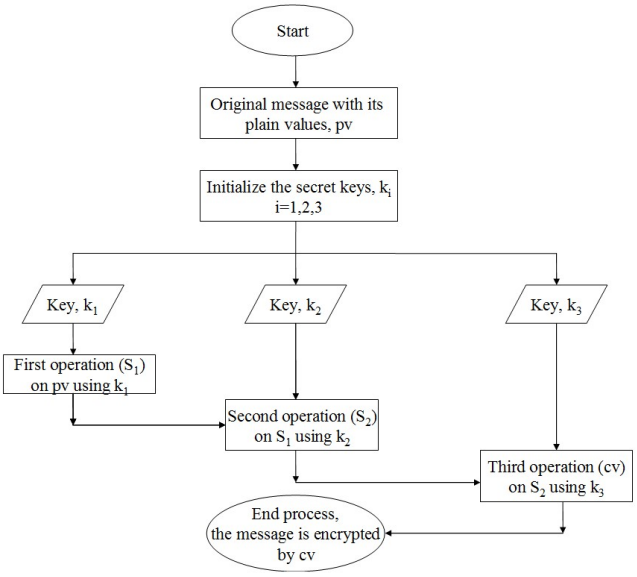

Figure 3. Illustration of Symmetric key encryption

Thus the given plaintext will be converted into the blocks of capital alphabets from A to J. The length of each block will vary with respect to the length of the keys used to encrypt the original message. The length of the three encryption keys is independent of length of plaintext. It should be noted that the there will be as many blocks as the characters of plaintext. The encrypted message (EM) will be quite difficult to break for the attacker as there will be no clue like frequency analysis. Meaning the original message may contain any symbol but the encrypted message will have always blocks containing only A, B, C, D, E, F, G, H, I, J.

$$T_1 = cv + k_3, \tag{4}$$

$$T_2 = T_1 - k_2, \tag{5}$$

$$T_3 = \frac{T_2}{k_3} = pv. \tag{6}$$

Finally, label the to the symbols as given in the Table 1. Thus the original message will be recovered. The framework of the proposed decryption idea is exhibited by the following Figure 4.

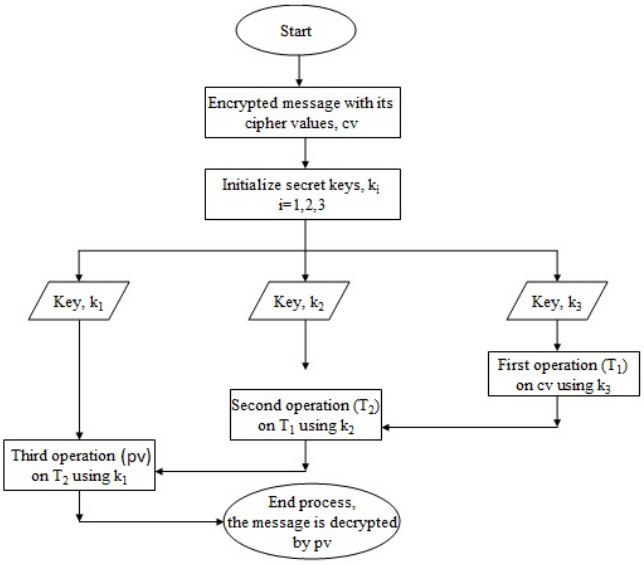

Figure 4. The proposed decryption algorithm

In order to check the correctness of the proposed encryption/decryption algorithm first of all the implementation steps were verified. Messages were tested for encryption/decryption. The encryption of secret message.

SM: Open the bank website http://www.banknp.com the user name is *BC*2016 and the password is my 20161516 banknp transfer 1 million US-dollar to this account 11562938 – 5 Encrypt the given message, by the using following keys *K*1 = 456654; *K*2 = 328975; and *K*3 = 7992:

Plaintext	Encryption by Different Ciphers				
	Proposed Algorithm	**DES**	**T-DES**	**IDEA**	**AES**
	Key:128bits k1= 456654----48bits k2= 328975----48bits k3= 7992-----32bits	Key:64bits (effectively 56bits) 00000006F7CE0000	Key:128bits (effectively 112 bits) 00000006F7CE0000 0005050F00001F38	Key:128bits 00000006F7CE0000 0005050F00001F38	Key:128bits 00000006F7CE0000 0005050F00001F38
O	HBHAHJD	8A	61	77	4B
p	BJFAAEFB	00	AE	DB	EB
e	BEEHHCFH	92	07	7D	B4
n	BIFIHBED	D7	4B	2C	54
	DCAJID	13	B9	EF	C2
t	CBDCHAGH	78	E1	0A	6A
h	BFIEHCBJ	D8	1F	23	B2
e	BEEHHCFH	4A	59	39	B6
	DCAJID	3A	9F	78	14
b	BDBAHCJF	0F	E9	CE	FA
a	BCGFAGEB	19	E0	C5	8E
n	BIFIHBED	49	34	BA	D6
k	BHCBHBIB	19	FA	B3	B1
	DCAJID	7D	A1	1A	49
w	CCGJHACJ	9F	B3	55	2D
e	BEEHHCFH	45	43	D7	74
b	BDBAHCJF	19	C9	71	A1
s	CAIHAEBD	45	8F	0D	49
i	BGDADIHD	84	8B	23	2A
t	CBDCHAGH	E1	C9	AD	18
e	BEEHHCFH	F8	16	62	57
	DCAJID	55	F8	12	8A
h	BFIEHCBJ	51	BD	59	B7
t	CBDCHAGH	DC	28	4C	23
t	CBDCHAGH	43	95	7D	18
p	BJFAAEFB	8A	60	FE	DD
:	DHHGGGBB	DF	F9	7A	0D
/	EBEBJIED	2F	7A	75	C7
/	EBEBJIED	C4	A3	63	EE
w	CCGJHACJ	42	4A	26	D1
w	CCGJHACJ	9C	D3	B7	1E
w	CCGJHACJ	70	8A	C1	05
.	EAAEJIIB	86	77	D4	46
b	BDBAHCJF	15	8E	32	7D
a	BCGFAGEB	82	94	DB	9A
n	BIFIHBED	70	5E	14	0E
k	BHCBHBIB	74	23	44	DA
n	BIFIHBED	7D	AB	FC	3C
p	BJFAAEFB	74	62	81	32
.	EAAEJIIB	6F	DB	23	58
c	BDFGDJEJ	83	D6	F1	57
o	BJAEDHJH	FB	D9	E2	F3
m	BIBDAEIJ	B8	EB	D7	32
	DCAJID	58	03	E2	C4

t	CBDCHAGH	56	B3	9A	82
h	BFIEHCBJ	DA	4A	9E	19
e	BEEHHCFH	8B	86	3F	FA
	DCAJID	16	CF	A6	68
u	CBHIDHCB	7F	AC	FE	BD
s	CAIHAEBD	A2	DC	DB	05
e	BEEHHCFH	51	F3	36	EB
r	CAEBDHFJ	D8	98	C5	EB
	DCAJID	DF	22	D8	54
n	BIFIHBED	7D	B2	8C	F3
a	BCGFAGEB	38	7A	31	B4
m	BIBDAEIJ	5D	3E	8E	88
e	BEEHHCFH	B0	54	61	DB
	DCAJID	1F	66	55	78
i	BGDADIHD	2E	E4	07	7A
s	CAIHAEBD	56	EA	92	73
	DCAJID	61	E4	AE	D5
B	BCDECJB	83	EC	72	8F
C	BGJAJEF	50	55	52	01
2	CFEDGJFD	42	33	5B	14
0	CEFCDGEF	E9	FF	52	F9
1	CEJIACJJ	3F	67	AA	CE
6	CHCGDFGJ	A6	A1	84	2B
	DCAJID	8A	16	9F	CC
a	BCGFAGEB	A6	06	6F	6B
n	BIFIHBED	85	0A	92	78
d	BEACAGAD	8B	63	6D	A3
	DCAJID	F8	EC	05	81
t	CBDCHAGH	63	68	E3	BF
h	BFIEHCBJ	88	05	72	21
e	BEEHHCFH	88	45	3D	61
	DCAJID	40	93	DB	51
p	BJFAAEFB	48	F7	02	B9
a	BCGFAGEB	16	16	BC	CD
s	CAIHAEBD	C9	59	20	A1
s	CAIHAEBD	07	A2	B5	A1
w	CCGJHACJ	D4	66	06	D0
o	BJAEDHJH	79	E2	1E	80
r	CAEBDHFJ	C0	32	EE	30
d	BEACAGAD	24	1B	B4	C3
	DCAJID	83	BB	CF	51
i	BGDADIHD	A9	DA	56	07
s	CAIHAEBD	2A	10	31	79
	DCAJID	F9	E9	49	0F
m	BIBDAEIJ	37	42	AF	C4
y	CDGBADDH	58	7E	4D	D2
2	CFEDGJFD	E8	E5	DA	8F
0	CEFCDGEF	E6	84	23	82
1	CEJIACJJ	33	DE	C2	CC
6	CHCGDFGJ	AC	82	2C	1D
1	CEJIACJJ	46	21	68	88
5	CGIAGJBF	E9	E0	46	90
1	CEJIACJJ	5A	8F	5B	D6
6	CHCGDFGJ	D6	44	49	0C
b	BDBAHCJF	A0	AF	61	B5
a	BCGFAGEB	E6	EC	68	D0
n	BIFIHBED	32	C3	24	CB
k	BHCBHBIB	04	16	E1	C4
n	BIFIHBED	52	2B	EE	86
p	BJFAAEFB	3B	7B	BD	2E
	DCAJID	61	31	79	7E

t	CBDCHAGH	74	92	75	00
r	CAEBDHFJ	FA	FC	48	06
a	BCGFAGEB	C1	62	75	78
n	BIFIHBED	46	3E	AD	AA
s	CAIHAEBD	7C	4A	96	FE
f	BEJDDJBB	62	8D	87	28
e	BEEHHCFH	91	95	FE	40
r	CAEBDHFJ	DC	7C	2D	18
	DCAJID	4B	90	8F	B4
l	CEJIACJJ	37	C8	06	78
	DCAJID	3D	16	9F	40
m	BIBDAEIJ	0D	F0	BE	35
i	BGDADIHD	9C	B5	79	3B
l	BHGHDIDF	F6	88	0A	9A
l	BHGHDIDF	B6	40	3F	6B
i	BGDADIHD	C2	1A	92	00
o	BJAEDHJH	BF	7E	3E	0C
n	BIFIHBED	EB	71	C2	81
	DCAJID	01	2F	E5	63
U	JJBAHBH	D7	24	5D	33
S	IJJHEAJ	C4	51	40	36
$	DAEGABEH	65	4C	CF	A7
	DCAJID	56	DC	88	02
t	CBDCHAGH	89	16	91	68
o	BJAEDHJH	AB	C1	B5	35
	DCAJID	84	56	05	30
t	CBDCHAGH	C9	52	46	8C
h	BFIEHCBJ	F1	1C	EC	33
i	BGDADIHD	DC	EC	F2	0A
s	CAIHAEBD	89	39	9C	A9
	DCAJID	2B	40	1F	0C
a	BCGFAGEB	E9	77	EC	1B
c	BDFGDJEJ	33	7C	7C	FB
c	BDFGDJEJ	FD	3D	A0	DC
o	BJAEDHJH	69	FC	FF	A2
u	CBHIDHCB	74	DB	18	BE
n	BIFIHBED	D2	94	B7	18
t	CBDCHAGH	B0	4D	D8	EF
	DCAJID	3E	4A	7A	BD
l	CEJIACJJ	D5	10	DF	25
l	CEJIACJJ	49	61	9F	6D
l	CEJIACJJ	B5	1F	1B	77
5	CGIAGJBF	B1	8B	BD	85
6	CHCGDFGJ	67	11	64	D2
2	CFEDGJFD	CA	F8	A8	7B
9	CIGDDFDB	BD	9D	23	08
3	CFIJDGAH	D9	62	9C	ED
8	CIBHGIHH	B6	80	81	A0
-	DEBBDDHJ	1C	66	6C	43
5	CGIAGJBF	89	CF	80	1B
.	EAAEJIIB	81	89	8C	BF
		4D	C9	58	83
		7B	E8	38	EB
		D6	7F	6C	E5
		56	84	F4	2A

Table 2. Encryption output of SM by proposed algorithm and its comparison with some modern symmetric key encryption methods

Decryption by Different Ciphers									
Proposed Algorithm		**DES**		**T-DES**		**IDEA**		**AES**	
Key:128bits k1= 456654----48bits k2= 328975----48bits k3= 7992-----32bits	**Recovered Plaintext**	Key:64bits (effectively 56bits) 00000006F7CE0000	**Recovered Plaintext**	Key:128bits (effectively 112 bits) 00000006F7CE0000 0005050F00001F38	**Recovered Plaintext**	Key:128bits 00000006F7CE0000 0005050F00001F38	**Recovered Plaintext**	Key:128bits 00000006F7CE0000 0005050F00001F38	**Recovered Plaintext**
Ciphertext		**Ciphertext**		**Ciphertext**		**Ciphertext**		**Ciphertext**	
HBHAHJD	**O**	8A	**O**	61	**O**	77	**O**	4B	**O**
BJFAAEFB	**p**	00	**p**	AE	**p**	DB	**p**	EB	**p**
BEEHHCFH	**e**	92	**e**	07	**e**	7D	**e**	B4	**e**
BIFIHBED	**n**	D7	**n**	4B	**n**	2C	**n**	54	**n**
DCAJID		13		B9		EF		C2	
CBDCHAGH	**t**	78	**t**	E1	**t**	0A	**t**	6A	**t**
BFIEHCBJ	**h**	D8	**h**	1F	**h**	23	**h**	B2	**h**
BEEHHCFH	**e**	4A	**e**	59	**e**	39	**e**	B6	**e**
DCAJID		3A		9F		78		14	
BDBAHCJF	**b**	0F	**b**	E9	**b**	CE	**b**	FA	**b**
BCGFAGEB	**a**	19	**a**	E0	**a**	C5	**a**	8E	**a**
BIFIHBED	**n**	49	**n**	34	**n**	BA	**n**	D6	**n**
BHCBHBIB	**k**	19	**k**	FA	**k**	B3	**k**	B1	**k**
DCAJID		7D		A1		1A		49	
CCGJHACJ	**w**	9F	**w**	B3	**w**	55	**w**	2D	**w**
BEEHHCFH	**e**	45	**e**	43	**e**	D7	**e**	74	**e**
BDBAHCJF	**b**	19	**b**	C9	**b**	71	**b**	A1	**b**
CAIHAEBD	**s**	45	**s**	8F	**s**	0D	**s**	49	**s**
BGDADIHD	**i**	84	**i**	8B	**i**	23	**i**	2A	**i**
CBDCHAGH	**t**	E1	**t**	C9	**t**	AD	**t**	18	**t**
BEEHHCFH	**e**	F8	**e**	16	**e**	62	**e**	57	**e**
DCAJID		55		F8		12		8A	
BFIEHCBJ	**h**	51	**h**	BD	**h**	59	**h**	B7	**h**
CBDCHAGH	**t**	DC	**t**	28	**t**	4C	**t**	23	**t**
CBDCHAGH	**t**	43	**t**	95	**t**	7D	**t**	18	**t**
BJFAAEFB	**p**	8A	**p**	60	**p**	FE	**p**	DD	**p**
DHHGGGBB	**:**	DF	**:**	F9	**:**	7A	**:**	0D	**:**
EBEBJIED	**/**	2F	**/**	7A	**/**	75	**/**	C7	**/**
EBEBJIED	**/**	C4	**/**	A3	**/**	63	**/**	EE	**/**
CCGJHACJ	**w**	42	**w**	4A	**w**	26	**w**	D1	**w**
CCGJHACJ	**w**	9C	**w**	D3	**w**	B7	**w**	1E	**w**
CCGJHACJ	**w**	70	**w**	8A	**w**	C1	**w**	05	**w**
EAAEJIIB	**.**	86	**.**	77	**.**	D4	**.**	46	**.**
BDBAHCJF	**b**	15	**b**	8E	**b**	32	**b**	7D	**b**
BCGFAGEB	**a**	82	**a**	94	**a**	DB	**a**	9A	**a**
BIFIHBED	**n**	70	**n**	5E	**n**	14	**n**	0E	**n**
BHCBHBIB	**k**	74	**k**	23	**k**	44	**k**	DA	**k**
BIFIHBED	**n**	7D	**n**	AB	**n**	FC	**n**	3C	**n**
BJFAAEFB	**p**	74	**p**	62	**p**	81	**p**	32	**p**
EAAEJIIB	**.**	6F	**.**	DB	**.**	23	**.**	58	**.**
BDFGDJEJ	**c**	83	**c**	D6	**c**	F1	**c**	57	**c**
BJAEDHJH	**o**	FB	**o**	D9	**o**	E2	**o**	F3	**o**
BIBDAEIJ	**m**	B8	**m**	EB	**m**	D7	**m**	32	**m**
DCAJID		58		03		E2		C4	
CBDCHAGH	**t**	56	**t**	B3	**t**	9A	**t**	82	**t**
BFIEHCBJ	**h**	DA	**h**	4A	**h**	9E	**h**	19	**h**
BEEHHCFH	**e**	8B	**e**	86	**e**	3F	**e**	FA	**e**
DCAJID		16		CF		A6		68	
CBHIDHCB	**u**	7F	**u**	AC	**u**	FE	**u**	BD	**u**
CAIHAEBD	**s**	A2	**s**	DC	**s**	DB	**s**	05	**s**
BEEHHCFH	**e**	51	**e**	F3	**e**	36	**e**	EB	**e**
CAEBDHFJ	**r**	D8	**r**	98	**r**	C5	**r**	EB	**r**
DCAJID		DF		22		D8		54	
BIFIHBED	**n**	7D	**n**	B2	**n**	8C	**n**	F3	**n**
BCGFAGEB	**a**	38	**a**	7A	**a**	31	**a**	B4	**a**
BIBDAEIJ	**m**	5D	**m**	3E	**m**	8E	**m**	88	**m**
BEEHHCFH	**e**	B0	**e**	54	**e**	61	**e**	DB	**e**
DCAJID		1F		66		55		78	
BGDADIHD	**i**	2E	**i**	E4	**i**	07	**i**	7A	**i**
CAIHAEBD	**s**	56	**s**	EA	**s**	92	**s**	73	**s**
DCAJID		61		E4		AE		D5	

BCDECJB	B	83	B	EC	B	72	B	8F	B
BGJAJEF	C	50	C	55	C	52	C	01	C
CFEDGJFD	2	42	2	33	2	5B	2	14	2
CEFCDGEF	0	E9	0	FF	0	52	0	F9	0
CEJACJJ	1	3F	1	67	1	AA	1	CE	1
CHCGDFGJ	6	A6	6	A1	6	84	6	2B	6
DCAJID		8A		16		9F		CC	
BCGFAGEB	a	A6	a	06	a	6F	a	6B	a
BIFIHBED	n	85	n	0A	n	92	n	78	n
BEACAGAD	d	8B	d	63	d	6D	d	A3	d
DCAJID		F8		EC		05		81	
CBDCHAGH	t	63	t	68	t	E3	t	BF	t
BFIEHCBJ	h	88	h	05	h	72	h	21	h
BEEHHCFH	e	88	e	45	e	3D	e	61	e
DCAJID		40		93		DB		51	
BJFAAEFB	p	48	p	F7	p	02	p	B9	p
BCGFAGEB	a	16	a	16	a	BC	a	CD	a
CAIHAEBD	s	C9	s	59	s	20	s	A1	s
CAIHAEBD	s	07	s	A2	s	B5	s	A1	s
CCGJHACJ	w	D4	w	66	w	06	w	D0	w
BJAEDHJH	o	79	o	E2	o	1E	o	80	o
CAEBDHFJ	r	C0	r	32	r	EE	r	30	r
BEACAGAD	d	24	d	1B	d	B4	d	C3	d
DCAJID		83		BB		CF		51	
BGDADIHD	i	A9	i	DA	i	56	i	07	i
CAIHAEBD	s	2A	s	10	s	31	s	79	s
DCAJID		F9		E9		49		0F	
BIBDAEIJ	m	37	m	42	m	AF	m	C4	m
CDGBADDH	y	58	y	7E	y	4D	y	D2	y
CFEDGJFD	2	E8	2	E5	2	DA	2	8F	2
CEFCDGEF	0	E6	0	84	0	23	0	82	0
CEJACJJ	1	33	1	DE	1	C2	1	CC	1
CHCGDFGJ	6	AC	6	82	6	2C	6	1D	6
CEJACJJ	1	46	1	21	1	68	1	88	1
CGIAGJBF	5	E9	5	E0	5	46	5	90	5
CEJACJJ	1	5A	1	8F	1	5B	1	D6	1
CHCGDFGJ	6	D6	6	44	6	49	6	0C	6
BDBAHCJF	b	A0	b	AF	b	61	b	B5	b
BCGFAGEB	a	E6	a	EC	a	68	a	D0	a
BIFIHBED	n	32	n	C3	n	24	n	CB	n
BHCBHBIB	k	04	k	16	k	E1	k	C4	k
BIFIHBED	n	52	n	2B	n	EE	n	86	n
BJFAAEFB	p	3B	p	7B	p	BD	p	2E	p
DCAJID		61		31		79		7E	
CBDCHAGH	t	74	t	92	t	75	t	00	t
CAEBDHFJ	r	FA	r	FC	r	48	r	06	r
BCGFAGEB	a	C1	a	62	a	75	a	78	a
BIFIHBED	n	46	n	3E	n	AD	n	AA	n
CAIHAEBD	s	7C	s	4A	s	96	s	FE	s
BEJDDJBB	f	62	f	8D	f	87	f	28	f
BEEHHCFH	e	91	e	95	e	FE	e	40	e
CAEBDHFJ	r	DC	r	7C	r	2D	r	18	r
DCAJID		4B		90		8F		B4	
CEJACJJ	1	37	1	C8	1	06	1	78	1
DCAJID		3D		16		9F		40	
BIBDAEIJ	m	0D	m	F0	m	BE	m	35	m
BGDADIHD	i	9C	i	B5	i	79	i	3B	i
BHGHDIDF	l	F6	l	88	l	0A	l	9A	l
BHGHDIDF	l	B6	l	40	l	3F	l	6B	l
BGDADIHD	i	C2	i	1A	i	92	i	00	i
BJAEDHJH	o	BF	o	7E	o	3E	o	0C	o
BIFIHBED	n	EB	n	71	n	C2	n	81	n
DCAJID		01		2F		E5		63	
JJBAHBH	U	D7	U	24	U	5D	U	33	U
IJJHEAJ	S	C4	S	51	S	40	S	36	S
DAEGABEH	$	65	$	4C	$	CF	$	A7	$
DCAJID		56		DC		88		02	
CBDCHAGH	t	89	t	16	t	91	t	68	t
BJAEDHJH	o	AB	o	C1	o	B5	o	35	o
DCAJID		84		56		05		30	
CBDCHAGH	t	C9	t	52	t	46	t	8C	t
BFIEHCBJ	h	F1	h	1C	h	EC	h	33	h
BGDADIHD	i	DC	i	EC	i	F2	i	0A	i
CAIHAEBD	s	89	s	39	s	9C	s	A9	s
DCAJID		2B		40		1F		0C	

BCGFAGEB	a	E9	a	77	a	EC	a	1B	a
BDFGDJEJ	c	33	c	7C	c	7C	c	FB	c
BDFGDJEJ	c	FD	c	3D	c	A0	c	DC	c
BIAEDHJH	o	69	o	FC	o	FF	o	A2	o
CBHIDHCB	u	74	u	DB	u	18	u	BE	u
BIFIHBED	n	D2	n	94	n	B7	n	18	n
CBDCHAGH	t	B0	t	4D	t	D8	t	EF	t
DCAJID		3E		4A		7A		BD	
CEJIACJJ	1	D5	1	10	1	DF	1	25	1
CEJIACJJ	1	49	1	61	1	9F	1	6D	1
CEJIACJJ	1	B5	1	1F	1	1B	1	77	1
CGIAGJBF	5	B1	5	8B	5	BD	5	85	5
CHCGDFGJ	6	67	6	11	6	64	6	D2	6
CFEDGJFD	2	CA	2	F8	2	A8	2	7B	2
CIGDDFDB	9	BD	9	9D	9	23	9	08	9
CFIJDGAH	3	D9	3	62	3	9C	3	ED	3
CIBHGIHH	8	B6	8	80	8	81	8	A0	8
DEBBDDHJ	-	1C	-	66	-	6C	-	43	-
CGIAGJBF	5	89	5	CF	5	80	5	1B	5
EAAEJIB	.	81	.	89	.	8C	.	BF	.
		4D		C9		58		83	
		7B		E8		38		EB	
		D6		7F		6C		E5	
		56		84		F4		2A	

Table 3. Decryption output of SM by proposed algorithm and its comparison with some modern symmetric key encryption methods

It can be seen that, the input messages encrypted by the proposed algorithm with three different keys. Also it can be seen that the reverse of encryption is also true that is; decryption of the secret messages produces the original message successfully by deciphering the encrypted messages provided that the key is same as used in the encryption process, for SM. The proposed algorithm have also been verified and compared with modern methods like DES, T-DES, IDEA and AES. In a similar fashion, the input message SM. The main difference in the working principle of the proposed algorithm and the other modern algorithms is that the proposed algorithm converts each character of secret message into the blocks of capital alphabets from A to J by considering the input keys into hexadecimal bits while the other modern ciphers convert each letter of the secret message into a block of a pair of hexadecimal characters having size (4+4) bits. Also the length of the encrypted message in modern methods is a multiple of 8 because the modern methods work on S-box (8x8 square matrix). Thus, it is very clear that the proposed algorithm is quite novel in terms of simplicity, variable block size as well as the consistency in the length of message during encryption and decryption processes.

5 PERFORMANCE METRICS

1:-Computational time (sec)

2:- Memory space utilization (bytes)

Computational time: The encryption/decryption time (in seconds) is the time taken by a computer to process the encryption/decryption algorithm. In order to evaluate and compare the encryption/decryption time taken by the proposed algorithm the Intel Core M-5Y10c CPU, with 0.8 GHz-1.00 GHz processor, 4 GB RAM, Windows 8 64 bit operating system and MATLAB computational resources are used. In this section the encryption/decryption time taken by the proposed algorithm is analyzed and compared with the some modern symmetric key algorithms, exhibits the encryption time taken by proposed algorithm to encrypt secret message SM. In order to test the advanced efficiency of the proposed encryption/decryption algorithm its computational time is compared with modern symmetric key encryption methods. The enhancement in the efficiency in terms of computational time in the proposed algorithm can be observed

in the Fig 5. reveals that proposed algorithm takes less encryption for input message as compared to the modern symmetric key encryption algorithms DES, T-DES, IDEA and AES. The T-DES takes highest encryption time while the encryption time of AES is near to the encryption time of the proposed algorithm but the implementation of AES is based on complicated process. Similarly, Fig 6. exhibits the decryption time of proposed algorithm in comparison with modern symmetric key algorithms. It can been seen that the decryption time taken by the proposed algorithm is less than other algorithms for input message.

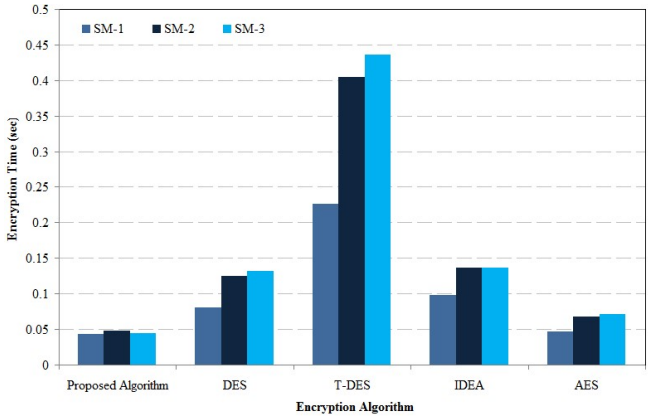

Figure 5. Comparison of computational time analysis of proposed encryption algorithm with some modern algorithm

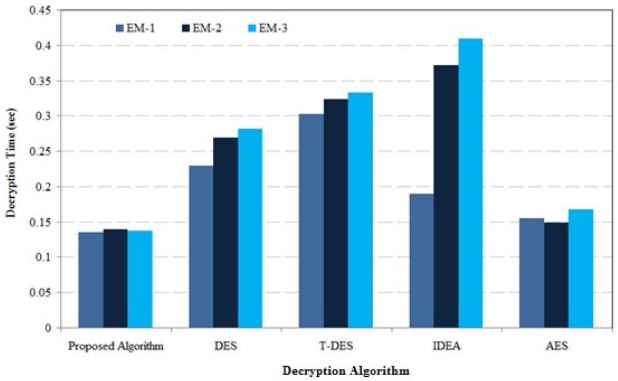

Figure 6. Comparison of computational time analysis of proposed decryption algorithm with some modern algorithm

Memory Space Utilization: The each given plaintext or ciphertext occupies space in computer memory. Each character in text takes 8 bytes of memory, for example; a plaintext having size 100 characters including alphabets, numbers, special symbols and blank spaces will occupy $8x100 = 800$ bytes in memory. The memory utilization may or may not be the same in encryption and decryption algorithms respectively. In this section the encryption/decryption memory usage (in bytes) by the proposed algorithm and some modern symmetric key algorithms is tested. In order to achieve this goal the same computational resources used as discussed in the above section. The figure. analyzes the memory usage by proposed algorithm to encrypt secret messages SM, and comparison with modern symmetric key encryption methods. It is again seen that in Fig 7. the proposed algorithm takes more memory usage in terms of encryption

algorithm as compared to some modern algorithms, DES, T-DES, IDEA and AES. This is again better accuracy and performance of the proposed algorithm. And evaluation of decrypted data blocks of ciphertext takes equal memory utilization of the proposed algorithm as well as modern decryption algorithms DES, T-DES, IDEA and AES, which is exhibited in the Figure 8.

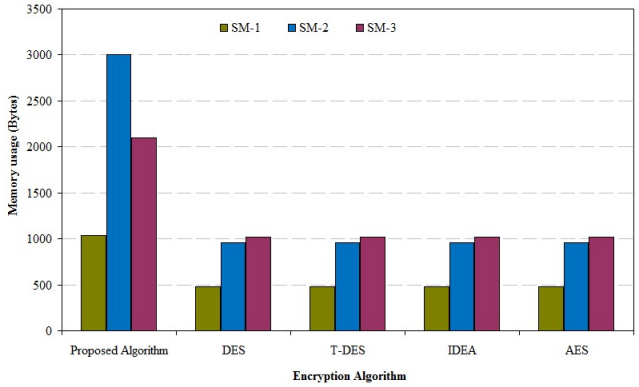

Figure 7. Comparison of memory usage in proposed encryption algorithm with some modern algorithm

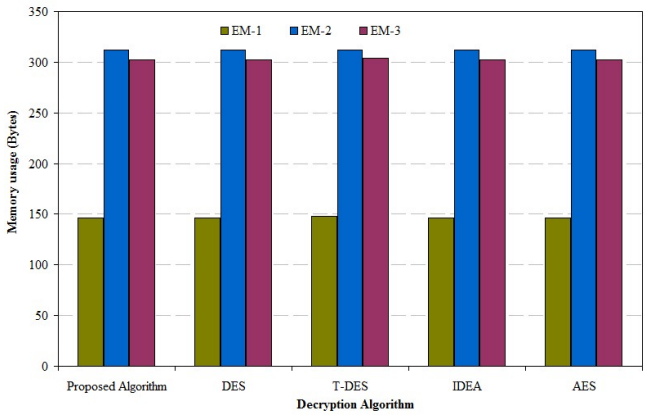

Figure 8. Comparison of memory usage in proposed decryption algorithm with some modern algorithm

6 conclusion

A symmetric key encryption/decryption algorithm is developed which is based on the idea of stream and blocks ciphers in which the encrypted message is converted into blocks of capital alphabets of English from A-J. The algorithm is very simple in terms of mathematical operations as it uses only arithmetic operations and does not use modular arithmetic, matrices or other complicated mathematical operations. One of the special features of developed algorithm is that it is not limited on just 26 English alphabets but can be applied efficiently to encrypt the secret messages containing the numbers, punctuations, elementary mathematics operations and special characters. Also, there is no limit of keys for encryption/decryption of the messages because the algorithm works well for all keys K_1; K_2; and $K3$; $K_2 \geq K_3$; taken from $N = 1, 2, 3$. Thus the probability of brute force attack is very small.

Author Contributions

Shakeel Ahmed Kamboh as first author wrote first draft of the manuscript, designed the study and whole supervision. **Suhail Ahmed Khaskheli** reviewed the relevant literature and analysis of the study. **Abbas Ali Ghoto** designed the methodology and performed simulations.**Sunny Kumar Aasoori** reviewing and writing. **Muzaffar Bashir Arain** editing and final revision of the manuscript.

8 Compliance with Ethical Standards

It is declare that all authors don't have any conflict of interest.

Funding Information

Author Information

ORCID:
Shakeel Ahmed Kamboh: 0000-0002-3468-1663
Abbas Ali Ghoto: 0000-0003-1243-3690

7 Reference

[1] Sharma, S.J., The Art of Cryptography: From Ancient Number System to Strange Number System. International Journal of Application or Innovation in Engineering and management (IJAIEM), ISSN, pp.2319-4847.

[2] Wasnik, T.P., Patil, V.S., Patinge, S.A., Dave, S.R. and Sayasikamal, G.J., 2013. Cryptography as an instrument to network security||. International Journal of Application or Innovation in Engineering Management (IJAIEM), 2(3), pp.72-80.

[3] Al-Vahed, A. and Sahhavi, H., 2011. An overview of modern cryptography. World Applied Programming, 1(1), pp.55-61.

[4] Ritu Tripathi, and Sanjay Agrawal., (2014). Comparative Study of Symmetric and Asymmetric Cryptography Techniques International Journal of Advance Foundation and Research in Computer (IJAFRC), 1(6), pp. 68-76.

[5] Alam, M.I. and Khan, M.R., 2013. Performance and efficiency analysis of different block cipher algorithms of symmetric key cryptography. International Journal of Advanced Research in Computer Science and Software Engineering, 3(10), pp.713-720.

[6] Suguna, S., Dhanakoti, V. and Manjupriya, R., 2016. A study on symmetric and asymmetric key encryption algorithms. Int Res J Eng Technol (IRJET), 3(4), pp.27-31.

[7] Kumari, S., 2017. A research paper on cryptography encryption and compression techniques. International Journal Of Engineering And Computer Science, 6(4), pp.20915-20919.

[8] AbuTaha, M., Farajallah, M., Tahboub, R. and Odeh, M., 2011. Survey paper: cryptography is the science of information security.

[9] Thambiraja, E., Ramesh, G. and Umarani, D.R., 2012. A survey on various most common encryption techniques. International journal of advanced research in computer science and software engineering, 2(7).

[10] Poonia, P. and Kantha, P., 2016. Comparative Study of Various Substitution and Transposition Encryption Techniques. Int. J. Comput. Appl, 145(10), pp.24-27.

[11] Kenang Eko Prasetyol, Tito Waluyo Purboyo, and Randy Erfa Saputra,(2017). A Survey on Data Comparison and Cryptography Algorithms International Journal of Applied Engineering Research (IJAER), 12(23), pp. 13589-13595.
[12] Shyam Nandan Kumar. Review on Network Security and Cryptography International Transaction of Electrical and Computer Engineers System (ITECE), Vol. 3, No. 1, ISSN (Online) 2373-1281 and ISSN (Print) 2373- 1273, (2015) pp.1-11.
[13] Saranya, K., Mohanapriya, R. and Udhayan, J., 2014. A review on symmetric key encryption techniques in cryptography. International Journal of Science, Engineering and Technology Research (IJSETR), 3(3), pp.539-544.
[14] Mohan, M., Devi, M.K. and Prakash, V.J., 2015. Security analysis and modification of classical encryption scheme. Indian journal of science and technology, 8(8), pp.542-548.
[15] Kendhe, A.K. and Agrawal, H., 2013. A survey report on various cryptanalysis techniques. International Journal of Soft Computing and Engineering (IJSCE), 3(2), pp.287-293.
[16] Dave, K.T., 2013. Brute-force Attack 'Seeking but Distressing'. Int. J. Innov. Eng. Technol. Brute-force, 2(3), pp.75-78.
[17] Mandal, P.C., 2012. Evaluation of performance of the Symmetric Key Algorithms: DES, 3DES, AES and Blowfish. Journal of Global Research in Computer Science, 3(8), pp.67-70.
[18] Mahajan, P. and Sachdeva, A., 2013. A study of encryption algorithms AES, DES and RSA for security. Global Journal of Computer Science and Technology.
[19] Masram, R., Shahare, V., Abraham, J. and Moona, R., 2014. Analysis and comparison of symmetric key cryptographic algorithms based on various file features. International Journal of Network Security Its Applications, 6(4), p.43.
[20] Rusia, M.K. and Rusia, M., 2017. A literature survey on efficiency and security of symmetric cryptography. Intern. J. of Comp. Sci. and Network, 6(3), pp.425-429.
[21] Mathur, H., 2015. Prof. Zahid Alam," Analysis In Symmetric And Asymmetric Cryptology Algorithm". International Journal of Emerging Trends Technology in Computer Science, 4(1), pp.44-47.
[22] Karthik, S. and Muruganandam, A., 2014. Data Encryption and Decryption by using Triple DES and performance analysis of crypto system. International Journal of Scientific Engineering and Research, 2(11), pp.24-31.
[23] Zoran Herigonja, 2016. Comparative Analysis of Cryptographic Algorithms International Journal of Digital Technology and Economy (IJDTE),1(2), pp. 127-134.
[24] More, S., 2015. Implementation of AES with Time Complexity Measurement for Various Input. Global Journal of Computer Science and Technology, 15(E4), pp.11-20.
[25] B.Bharathi, G.Manivasagam, and M. Anand Kumar, 2017. Metrics for Performance Evaluation of Encryption Algorithms International Journal of Advance Research in Science and Engineering (IJARSE),6(3)pp. 62-72.