International Journal of Advances in Applied Sciences (IJAAS)
Vol. 8, No. 1, March 2019, pp. 44~53
ISSN: 2252-8814, DOI: 10.11591/ijaas.v8.i1.pp44-53

KED-AES algorithm: combined key encryption decryption and advance encryption standard algorithm

Edwin R. Arboleda, Carla Eunice R. Fenomeno, Joshua Z. Jimenez
Department of Computer and Electronics Engineering, College of Engineering and Information Technology,
Cavite State University, Philippines

Article Info

Article history:

Received Nov 21, 2018
Revised Jan 16, 2019
Accepted Feb 1, 2019

Keywords:

Advance encryption standard
Cryptography
Key encryption decryption

ABSTRACT

Two existing cryptosystems are being combined and proposed. It is the enhanced combination of KED (Key Encryption Decryption), a cryptosystem that uses modulo 69 and the AES (Advance Encryption Standard) cryptography. The strength of the KED is that the keys are being used by the sender and the receiving end. The AES is easy to implement and has good defense against various attacks such as hacking.

Corresponding Author:

Edwin R. Arboleda,
Department of Computer and Electronics Engineering,
College of Engineering and Information Technology, Cavite State University,
Indang, Cavite, Philippines.
Email: edwin.r.arboleda@cvsu.edu.ph

1. INTRODUCTION

Cryptography is the science of encrypting and decrypting information. It is the art of securing data or information by transforming it into another unreadable format wherein a message is hidden from anyone who will read it and only the intended receiver will be able to convert it and reveal the hidden message. The main goal of cryptography is to secure the data from illegal access [1, 2].

Based on [3, 4], it stated that Cryptography is the scientific establishment on which one forms secure frameworks. It contemplates methods for safely putting away, transmitting, and handling data. Understanding what cryptographic primitives can do, and how they can be made together, is important to construct secure frameworks, however not enough. A few extra contemplations go into the outline of secure frameworks, and they are secured in different Berkeley graduate courses on security [2].

Cryptography is about correspondence within the sight of an enemy. It includes numerous issues (encryption, verification, key appropriation to give some examples). The field of current cryptography gives a hypothetical establishment considering which we may comprehend what precisely these issues are, the manner by which to assess conventions that indicate to explain them, and how to construct conventions in whose security we can have. We present the essential issues by talking about the issue of encryption [5].

According to [6], Cryptography is the place security designing meets arithmetic. It gives us the apparatuses that underlie most advanced security conventions. It is presumably the key empowering innovation for securing appropriated frameworks, yet it is shockingly difficult to do right. "Conventions," cryptography has frequently been utilized to secure the wrong things or used to ensure them in the wrong way. We'll see bounty more cases when we begin looking in detail at genuine applications [7].

Cryptography is the exploration of writing in mystery code and is an antiquated craftsmanship; the initially reported utilization of cryptography in composing goes back to around 1900 B.C. at the point when an Egyptian copyist utilized non-standard symbolic representations as a part of an engraving [8]. A few specialists contend that cryptography showed up suddenly at some point in the wake of composing was developed, with applications running from strategic letters to war-time fight arranges. It is nothing unexpected, then, that new types of cryptography came not long after the broad improvement of PC correspondences [9]. In information and broadcast communications, cryptography is fundamental when imparting over any untrusted medium, which incorporates pretty much any system, especially the internet [8].

There are two basic types of encryption, symmetric algorithm and asymmetric algorithm. According to [10] symmetric algorithms also called “secret key” uses the same key for both encryption and decryption and asymmetric algorithms or “public key” uses different keys for encryption and decryption [11]. A symmetric cryptosystem (or private key cryptosystem) utilizes one and only key for both encryption and unscrambling of the information. The key utilized for encryption and unscrambling is called the private key and just individuals who are approved for the encryption/unscrambling would know it. In a symmetric cryptosystem, the encoded message is sent over without any open keys joined to it while asymmetric or the public key there are two distinctive keys utilized for the encryption and decoding of information [8]. The key utilized for encryption is kept open thus as called open key, and the unscrambling key is kept mystery and called private key. The keys are created in a manner that it is difficult to get the private key from people in general key. The transmitter and the beneficiary both have two keys in an Asymmetric framework. Be that as it may, the private key is kept private and not sent over with the message to the beneficiary, in spite of the fact that the general population key is this is further explained by [11].

The advantages and disadvantages of symmetric and asymmetric cryptosystem was stated by [12], A symmetric cryptosystem is speedier, encoded information be exchanged on the connection regardless of the possibility that there is a probability that the information will be caught. Since there is no key transmitted with the information, the odds of information being decoded are invalid, it utilizes secret word validation to demonstrate the beneficiary's character and a framework just which has key can unscramble a message are the benefits of symmetric cryptosystem while in Asymmetric cryptosystem [13], cryptography there is no requirement for trading keys, along these lines wiping out the key conveyance issue [14], the essential preferred standpoint of open key cryptography is expanded security: the private keys absolutely never should be transmitted or uncovered to anybody, and in conclusion it can give advanced marks that can be denied [15]. The disadvantages of symmetric cryptosystem have an issue of key transportation. The private key is to be transmitted to the getting framework before the real message is to be transmitted [16, 17]. Each method for electronic correspondence channels. In this way, the main secure method for trading keys would trade them by and by and can't give advanced mark that can't be revoked. While in asymmetric cryptosystem an impediment of utilizing open key cryptography for encryption is speed: there are well known mystery key encryption techniques which are altogether speedier than any right now accessible open key encryption strategy [18].

This standard indicates the Rijndael calculation [19, 20], a symmetric square figure that can prepare information squares of 128 bits, utilizing figure keys with lengths of 128, 192, and 256 bits [21]. Rijndael was intended to handle extra piece sizes and key lengths, nonetheless they are not embraced in this standard. All through the rest of this standard, the calculation determined thus will be alluded to as "the AES algorithm." The algorithm might be utilized with the three different key lengths, mention above, and in this way, these different "flavors" might be alluded to as "AES-128", "AES-192", and"AES-256 [4]".

Warjri [22] proposed a new symmetric key algorithm called as KED (Key Encryption Decryption) and a new key generation method. Using modulo 69 and inverse modulo69, the proposed algorithm was used for encryption and decryption process, in which the same key is used both for encryption and decryption.

2. RESEARCH METHOD

The authors proposed a hybrid of KED that uses modulo 69, CHAOS-based cryptosystem, and AES algorithm. The key generation used in this hybrid uses that of KED and all the algorithm are used in encryption and decryption process [18]. The s-box and inverse s-box tables will be used in encryption and decryption respectively; they will be part of the process itself and not in the sent message. The Encryption process is shown in Figure 1 and The Decryption process is shown in Figure 2.

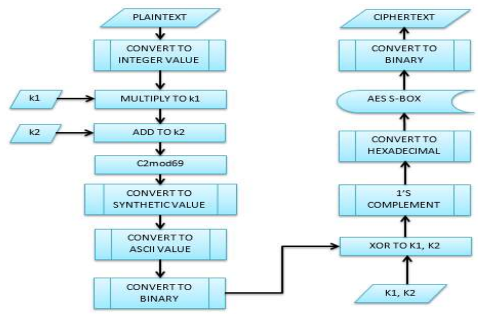

Figure 1. Encryption process

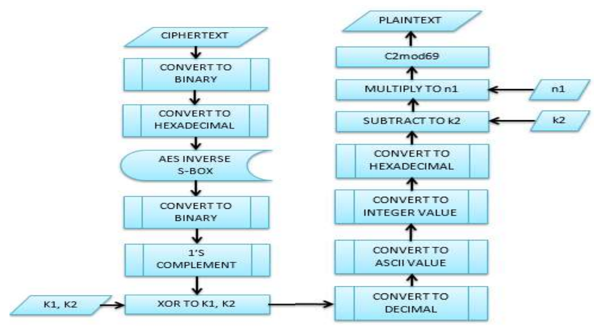

Figure 2. Decryption process [23]

Key generation algorithm
KED Key Generation:

a. Generating 'k2', firstly user enters a key. The length of the key is stored in 'kl'. Hence k2 is generated as follows:

   $K2=(\sum_{i=0}^{kl-1} 2^{i} * kl * val) \bmod m$

b. Where, 'i' is the position of each character in the key. 'kl' is the length of the key. 'val' is the integer value that has been assign to each character as shown in Figure 3.

c. For 'k1', select any natural number say 'k1' where k1≠0 and must be relatively prime to 'm' (i.e., 'k1' should not have factors in common with 'm').

d. Find inverse modulo69 of 'k1' and store it in 'n1'

Chaos Key Generation:

a. Convert k1 and k2 to its 8-bit binary equivalent.
b. Get the gray code of the binary form of k1 and k2, denote as J1 and J2.

Encryption
KED:

A	B	C	D	E	F	G	H	I
1	2	3	4	5	6	7	8	9
J	K	L	M	N	O	P	Q	R
10	11	12	13	14	15	16	17	18
S	T	U	V	W	X	Y	Z	0
19	20	21	22	23	24	25	26	27
1	2	3	4	5	6	7	8	9
28	29	30	31	32	33	34	35	36
space	!	"	#	$	%	&	'	(
37	38	39	40	41	42	43	44	45
)	*	+	,	-	.	/	:	;
46	47	48	49	50	51	52	53	54
<	=	>	?	@	[	\	]	^
55	56	57	58	59	60	61	62	63
_	`	{	|	}	~			
64	65	66	67	68	69			

Figure 3. Synthetic values of alphabets [23]

a. Firstly, substitute or assign integer value for plain text.
b. Multiply Synthetic value with first key i.e., k1.
c. Now add the result from step 2 above with second key i.e., k2.
d. Then calculate with modulo69.

CHAOS:
a. Convert mi to 8-bit binary equivalent.
b. XOR the 8-bit binary with the corresponding k.
c. Get the 1's complement, denoted as w.

AES:
a. Convert the binary to hexadecimal
b. Apply the S-box to each value as shown in Figure 4, denoted as W1.
c. The first digit will be the row x, and second digit will be the column y.
d. Convert to binary the row x and column y.
e. Convert to decimal the 8-bit binary for the cipher text.

x \ y	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	db	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

Figure 4. AES S-Box [23]

Decryption

AES:
a. Convert to binary to hexadecimal.
b. Apply the inverse S-box as shown in Figure 5, denoted as W2.
c. Covert to binary.

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

Figure 5. AES Inverse S-Box [23]

CHAOS:
a. Get the 1's complement, denoted as 'S'.
b. XOR the 8-bit binary with the corresponding k.
c. Convert the 8-bit binary to its decimal equivalent, denoted as mi.
KED:
a. Assign integer value for cipher text as given in Figure 3.
b. Subtract 'k2' from above integer value.
c. Multiply above result with inverse modulo69 of 'k1' i.e., 'n1'.
d. Finally calculate with modulo69.

3. RESULTS AND ANALYSIS

Message: COZY LOOBY GIVES SHARP SQUID WHO ASK FOR JOB PEN. The Encryption and Decryption are shown in Table 1-6.
Encryption:

Table 1. KED encryption

Plaintext (PT)	Integer Value (V1)	V1*K1 (C1)	C1+K2 (C2)	C2 mod69	Synthetic Value
C	3	15	21	21	U
O	15	75	81	12	L
Z	26	130	136	67	|
Y	25	125	131	62	]
SPACE	37	185	191	53	:
L	12	60	66	66	{
O	15	75	81	12	L
O	15	75	81	12	L
B	2	10	16	16	P
Y	25	125	131	62	]
SPACE	37	185	191	53	:
G	7	35	41	41	$
I	9	45	51	51	.
V	22	110	116	47	*
E	5	25	31	31	4
S	19	95	101	32	5
SPACE	37	185	191	53	:
S	19	95	101	32	5
H	8	40	46	46	)
A	1	5	11	11	K
R	18	90	96	27	0
P	16	80	86	17	Q
SPACE	37	185	191	53	:
S	19	95	101	32	5
Q	17	85	91	22	V
U	21	105	111	42	%
I	9	45	51	51	.
D	4	20	26	26	Z
SPACE	37	185	191	53	:
W	23	115	121	52	/
H	8	40	46	46	(
0	15	75	81	12	U
SPACE	37	185	191	53	:
A	1	5	11	11	K
S	19	95	101	32	5
K	11	55	61	61	\
SPACE	37	185	191	53	:
F	6	30	36	36	9
O	15	75	81	12	U
R	18	90	96	27	0
SPACE	37	185	191	53	:
J	10	50	56	56	=
O	15	75	81	12	U
B	2	10	16	16	P
SPACE	37	185	191	53	:
P	16	80	86	17	Q
E	5	25	31	31	4
N	14	70	76	7	G
.	51	225	261	54	;

Table 2. CHAOS encryption

ASCII Value	Binary	Gray coded (K1 & K2)	XOR	1's Complement
85	0101 0101	0000 0111	0101 0010	1010 1101
76	0100 1100	0000 0101	0100 1001	1011 0110
124	0111 1100	0000 0111	0111 1011	1000 0100
93	0101 1101	0000 0101	0101 1000	1010 0111
58	0011 1010	0000 0111	0011 1101	1100 0010
123	0111 1010	0000 0101	0111 1110	1000 0001
76	0100 1100	0000 0111	0100 1011	1011 0100
76	0100 1100	0000 0101	0100 1001	1011 0110
80	0101 0000	0000 0111	0101 0111	1010 1000
93	0101 1101	0000 0101	0101 1000	1010 0111
58	0011 1010	0000 0111	0011 1101	1100 0010
36	0010 0100	0000 0101	0010 0001	1101 1110
46	0010 0100	0000 0111	0010 0011	1101 1100
42	0010 1010	0000 0101	0010 1111	1101 0000
52	0011 0100	0000 0111	0011 0011	1100 1100
53	0011 0101	0000 0101	0011 0000	1100 1111
58	0011 1010	0000 0111	0011 1101	1100 0010
53	0011 0101	0000 0101	0011 0000	1100 1111
41	0010 1001	0000 0111	0010 1110	1101 0001
75	0100 1011	0000 0101	0100 1110	1011 0001
48	0011 0000	0000 0111	0011 0111	1100 1000
81	0101 0001	0000 0101	0101 0100	1010 1000
58	0011 1010	0000 0111	0011 1101	1100 0010
53	0011 0101	0000 0101	0011 0000	1100 1111
66	0100 0010	0000 0111	0100 0101	1011 1010
37	0010 0101	0000 0101	0010 0000	1101 1111
46	0010 0100	0000 0111	0010 0011	1101 1100
90	0101 1010	0000 0101	0101 1111	1010 0000
58	0011 1010	0000 0111	0011 1101	1100 0010
47	0010 1111	0000 0101	0010 1010	1101 0101
41	0010 1001	0000 0111	0010 1110	1101 0001
85	0101 0101	0000 0101	0101 0000	1010 1111
58	0011 1010	0000 0111	0011 1101	1100 0010
75	0100 1011	0000 0101	0100 1110	1011 0001
53	0011 0101	0000 0111	0011 0010	1100 1101
92	0101 1100	0000 0101	0101 1011	1010 0100
58	0011 1010	0000 0111	0011 1101	1100 0010
57	0011 1001	0000 0101	0011 1100	1100 0011
85	0101 0101	0000 0111	0101 0010	1010 1101
48	0011 0000	0000 0101	0011 0101	1100 1010
58	0011 1010	0000 0111	0011 1101	1100 0010
61	0011 1101	0000 0101	0011 1000	1100 0111
85	0101 0101	0000 0111	0101 0010	1010 1101
80	0101 0000	0000 0101	0101 0101	1010 1010
58	0011 1010	0000 0111	0011 1101	1100 0010
81	0101 0001	0000 0101	0101 0100	1010 1011
52	0011 0100	0000 0111	0011 0011	1100 1100
71	0100 0111	0000 0101	0100 0010	1011 1101
59	0011 1011	0000 0111	0011 1100	1100 0011

Table 3. AES encryption

Hexadecimal	AES S-Box (W1)	Binary	Cipher text
AD	95	1001 0101	149
B6	4e	0100 1110	78
84	5f	0101 1111	95
A7	5c	0101 1100	92
C2	25	0010 0101	37
81	0c	0000 1100	12
B4	8d	1000 1101	141
B6	4e	0100 1110	78
A8	c2	1100 0010	194
A7	5c	0101 1100	92
C2	2e	0010 1110	46
DE	1d	0001 1101	29
DC	86	1000 0110	134
D0	70	0111 0000	112
CC	4b	0100 1011	75
CF	8a	1000 1010	138
C2	25	0010 0101	37

Table 3. AES encryption (*continued*)

Hexadecimal	AES S-Box (W1)	Binary	Cipher text
CF	8a	1000 1010	138
D1	3e	0011 1110	62
B1	c8	1100 1000	200
C8	e8	1110 1000	232
A8	c2	1100 0010	194
C2	25	0010 0101	37
CF	8a	1000 1010	138
BA	f4	1111 0100	244
DF	9e	1001 1110	158
DC	86	1000 0110	134
A0	e0	1110 0000	224
C2	25	0010 0101	37
D5	03	0000 0011	3
D1	3e	0011 1110	62
AF	79	0111 1001	121
C2	25	0010 0101	37
B1	c8	1100 1000	200
CD	db	1101 1011	219
A4	49	0100 1001	73
C2	25	0010 0101	37
C3	2e	0010 1110	46
AD	95	1001 0101	149
CA	74	0111 0100	116
C2	25	0010 0101	37
C7	c6	1100 0110	198
AD	95	1001 0101	149
AA	ac	1010 1100	172
C2	25	0010 0101	37
AB	62	0110 0010	98
CC	4b	0100 1011	75
BD	7a	0111 1010	122
C3	2e	0010 1110	46

Decryption:

Table 4. AES decryption

Decimal	Binary	Hexadecimal	Inverse S-Box (W2)	Binary
149	1001 0101	95	AD	1010 1101
78	0100 1110	4e	B6	1011 0110
95	0101 1111	5f	84	1000 0100
92	0101 1100	5c	A7	1010 0111
37	0010 0101	25	C2	1100 0010
12	0000 1100	0c	81	1000 0001
141	1000 1101	8d	B4	1011 0100
78	0100 1110	4e	B6	1011 0110
194	1100 0010	c2	A8	1010 1000
92	0101 1100	5c	A7	1010 0111
46	0010 1110	2e	C2	1100 0010
29	0001 1101	1d	DE	1101 1110
134	1000 0110	86	DC	1101 1100
112	0111 0000	70	D0	1101 0000
75	0100 1011	4b	CC	1100 1100
138	1000 1010	8a	CF	1100 1111
37	0010 0101	25	C2	1100 0010
138	1000 1010	8a	CF	1100 1111
62	0011 1110	3e	D1	1101 0001
200	1100 1000	c8	B1	1011 0001
232	1110 1000	e8	C8	1100 1000
194	1100 0010	c2	A8	1010 1000
37	0010 0101	25	C2	1100 0010
138	1000 1010	8a	CF	1100 1111
244	1111 0100	f4	BA	1011 1010
158	1001 1110	9e	DF	1101 1111
134	1000 0110	86	DC	1101 1100
224	1110 0000	e0	A0	1010 0000
37	0010 0101	25	C2	1100 0010
3	0000 0011	03	D5	1101 0101
62	0011 1110	3e	D1	1101 0001

Table 4. AES decryption (*continued*)

Decimal	Binary	Hexadecimal	Inverse S-Box (W2)	Binary
121	0111 1001	79	AF	1010 1111
37	0010 0101	25	C2	1100 0010
200	1100 1000	c8	B1	1011 0001
219	1101 1011	db	CD	1100 1101
73	0100 1001	49	A4	1010 0100
37	0010 0101	25	C2	1100 0010
46	0010 1110	2e	C3	1100 0011
149	1001 0101	95	AD	1010 1101
116	0111 0100	74	CA	1100 1010
37	0010 0101	25	C2	1100 0010
198	1100 0110	c6	C7	1100 0111
149	1001 0101	95	AD	1010 1101
172	1010 1100	ac	AA	1010 1010
37	0010 0101	25	C2	1100 0010
98	0110 0010	62	AB	1010 1011
75	0100 1011	4b	CC	1100 1100
122	0111 1010	7a	BD	1011 1101
46	0010 1110	2e	C3	1100 0011

Table 5. CHAOS decryption

1's Complement (S)	J1 & J2	S XOR J1/J2 (S1)	Decimal	ASCII Code
0101 0010	0000 0111	0101 0101	85	U
0100 1001	0000 0101	0100 1100	76	L
0111 1011	0000 0111	0111 1100	124	|
0101 1000	0000 0101	0101 1101	93	]
0011 1101	0000 0111	0011 1010	58	:
0111 1110	0000 0101	0111 1010	123	{
0100 1011	0000 0111	0100 1100	76	L
0100 1001	0000 0101	0100 1100	76	L
0101 0111	0000 0111	0101 0000	80	P
0101 1000	0000 0101	0101 1101	93	]
0011 1101	0000 0111	0011 1010	58	:
0010 0001	0000 0101	0010 0100	36	$
0010 0011	0000 0111	0010 0100	46	.
0010 1111	0000 0101	0010 1010	42	*
0011 0011	0000 0111	0011 0100	52	4
0011 0000	0000 0101	0011 0101	53	5
0011 1101	0000 0111	0011 1010	58	:
0011 0000	0000 0101	0011 0101	53	5
0010 1110	0000 0111	0010 1001	41	)
0100 1110	0000 0101	0100 1011	75	K
0011 0111	0000 0111	0011 0000	48	0
0101 0100	0000 0101	0101 0001	81	Q
0011 1101	0000 0111	0011 1010	58	:
0011 0000	0000 0101	0011 0101	53	5
0100 0101	0000 0111	0100 0010	66	V
0010 0000	0000 0101	0010 0101	37	%
0010 0011	0000 0111	0010 0100	46	.
0101 1111	0000 0101	0101 1010	90	Z
0011 1101	0000 0111	0011 1010	58	:
0010 1010	0000 0101	0010 1111	47	/
0010 1110	0000 0111	0010 1001	41	(
0101 0000	0000 0101	0101 0101	85	U
0011 1101	0000 0111	0011 1010	58	:
0100 1110	0000 0101	0100 1011	75	K
0011 0010	0000 0111	0011 0101	53	5
0101 1011	0000 0101	0101 1100	92	\
0011 1101	0000 0111	0011 1010	58	:
0011 1100	0000 0101	0011 1001	57	9
0101 0010	0000 0111	0101 0101	85	U
0011 0101	0000 0101	0011 0000	48	0
0011 1101	0000 0111	0011 1010	58	:
0011 1000	0000 0101	0011 1101	61	=
0101 0010	0000 0111	0101 0101	85	U
0101 0101	0000 0101	0101 0000	80	P
0011 1101	0000 0111	0011 1010	58	:
0101 0100	0000 0101	0101 0001	81	Q
0011 0011	0000 0111	0011 0100	52	4
0100 0010	0000 0101	0100 0111	71	G
0011 1100	0000 0111	0011 1011	59	;

Table 6. KED decryption

Integer Value (V2)	V2-K2 (P1)	P1*n1 (P2)	P2 mod69	Plaintext (PT)
21	15	210	3	C
12	6	84	15	O
67	61	854	26	Z
62	56	784	25	Y
53	47	658	37	SPACE
66	60	840	12	L
12	6	84	15	O
12	6	84	15	O
16	10	140	2	B
62	56	784	25	Y
53	47	658	37	SPACE
41	35	490	7	G
51	45	630	9	I
47	41	574	22	V
31	25	350	5	E
32	26	364	19	S
53	47	658	37	SPACE
32	26	364	19	S
46	40	560	8	H
11	5	70	1	A
27	21	294	18	R
17	11	154	16	P
53	47	658	37	SPACE
32	26	364	19	S
22	16	224	17	Q
42	36	504	21	U
51	45	630	9	I
26	20	280	4	D
53	47	658	37	SPACE
52	46	644	23	W
46	40	560	8	H
12	6	84	15	O
53	47	658	37	SPACE
11	5	70	1	A
32	26	364	19	S
61	55	770	11	K
53	47	658	37	SPACE
36	30	420	6	F
12	6	84	15	O
27	21	294	18	R
53	47	658	37	SPACE
56	50	700	10	J
12	6	84	15	O
16	10	140	2	B
53	47	658	37	SPACE
17	11	154	16	P
31	25	350	5	E
7	1	14	14	N
54	48	672	51	.

4. CONCLUSION

The proposed cryptosystem was able to combine the KED using modulo 69, CHAOS-based and AES cryptosystem. It is the enhanced system of KED by adding the chaotic-based cryptosystem and the AES S-box and inverse S-box in both encryption and decryption. The proposed algorithm is then implemented by using a message that comprise the English alphabet. The key is generated using the proposed method. Then the message is encrypted and decrypted successfully.

REFERENCE

[1] S. Hebert, "A Brief History of Cryptography", an article [Online]. Available: http://cybercrimes.net/aindex.html.

[2] A. Sanada, Y. Nogami, K. Iokibe, and A. Khandaker, "Security Analysis of Raspberry Pi Against Side-Channel Attack with RSA Cryptography," pp. 287–288, 2017.

[3] Trevisan, L., "Cryptography. Lecture Notes from CS276," *Spring 2009*, vol. 154, 2009.

[4] L. K. Galla, V. S. Koganti, and N. Nuthalapati, "Implementation of RSA," in *2016 International Conference on Control Instrumentation Communication and Computational Technologies, ICCICCT 2016*, pp. 81–87, 2017.

[5] D. Llamocca, D. Ph, D. Debnath, D. Ph, L. Rong, and D. Ph, “Can Crypto Chip To Secure Data Transmitted Through Can Fd Bus by Using Aes-128 & Sha-1 With A Symmetric Key by Tri P. Doan," A dissertation submitted in partial fulfillment of the requirement for the degree of Doctor of Philosophy Rochester, Michigan Doct, 2017.
[6] Goldwasser, S., and Bellare, M., "Lecture Notes on Cryptography," 2008.
[7] S. Oukili and S. Bri, “High throughput FPGA Implementation of Data Encryption Standard with time variable sub-keys,” *Int. J. Electr. Comput. Eng.*, vol. 6, no. 1, p. 298, 2016.
[8] S. Dey, J. Nath, and A. Nath, “An Integrated Symmetric Key Cryptographic Method - Amalgamation of TTJSA Algorithm, Advanced Caesar Cipher Algorithm, Bit Rotation and Reversal Method: SJA Algorithm,” *Int. J. Mod. Educ. Comput. Sci.*, vol. 4, no. 5, pp. 1–9, 2012.
[9] P. K. Panda, “A Hybrid Security Algorithm for RSA Cryptosystem,” 2017.
[10] Caesar, G. J. and Kennedy, J.F. (n.d.)., "Cryptography. Security Engineering: A Guide to Building Dependable Distributed Systems," vol. 42, 2008.
[11] D. John and L. Martin, “Binary rsa encryption algorithm,” pp. 178–181, 2016.
[12] L. Kocarev, J.M. Amigo, and J. Szczepanski, “The Chaos-based Cryptography: an overview”, *IEEE Circuits and Systems Magazine*, vol. 1(3), pp. 6-21, 2001.
[13] Y. Chen, K. Li, X. Fei, Z. Quan, and K. Li, “Implementation and Optimization of AES Algorithm on the Sunway Taihu Light,” 2016.
[14] K. Garson, *Policy-Based Encryption and its Application in a Hospital System by*. 2009.
[15] Q. Zhang and A. Qunding, “Digital image encryption based on Advanced Encryption Standard(AES) algorithm,” *5th Int. Conf. Instrum. Meas. Comput. Commun. Control. IMCCC 2015*, pp. 1218–1221, 2015.
[16] J.-F. W. J.-F. Wang, S.-W. C. S.-W. Chang, and P.-C. L. P.-C. Lin, “A novel round function architecture for AES encryption/decryption utilizing look-up table,” *IEEE 37th Annu. 2003 Int. Carnahan Conf. onSecurity Technol. 2003 Proc.*, pp. 132–136, 2003.
[17] P. Katkade and G. M. Phade, “Application of AES algorithm for data security in serial communication,” *Proc. Int. Conf. Inven. Comput. Technol. ICICT 2016*, vol. 2016, 2016.
[18] O. A. Dawood, A. M. S. Rahma, and A. M. J. Abdul Hossen, “New Symmetric Cipher Fast Algorithm of Revertible Operations’ Queen (FAROQ) Cipher,” *Int. J. Comput. Netw. Inf. Secur.*, vol. 9, no. 4, pp. 29–36, 2017.
[19] J, Daemen and V. Rijmen, “AES Proposal: Rijndael, AES Algorithm Submission,” September 3, 1999.
[20] J. Daemen and V. Rijmen, “The block cipher Rijndael, Smart Card research and Applications, LNCS 1820,” *Springer-Verlag*, pp. 288-296.
[21] A. K. Sharma and H. Sharma, “New Approach to Des with Enhanced Key Management and Encryption/Decryption System,” vol. 32, pp. 1–31, 2012.
[22] J. Warjri, KED- “A Symmetric Key Algorithm for Secured Information Exchange Using Modulo 69*,” I.J Computer Network and Information Security*, vol. 10, pp 37-43, 2013.
[23] J. L. Lai, K. H. Liao, Y. Te Lai, and R. J. Chen, “Design CAROM module used in AES structure for Sub-Byte and Inv-Sub-Byte transformation,” *Proc. - 2013 Int. Symp. Biometrics Secur. Technol. ISBAST 2013*, no. 1, pp. 198–202, 2013.