ISSN No. 0976-5697

Volume 5, No. 3, March-April 2014

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Sea Encryption Algorithm for Information Security Using Code Sheet

N. Geethanjali
Assistant Professor
Department of Computer Science
Christ the King Engineering College

M. Ramya
Assistant Professor
Department of Computer Science
Christ the King Engineering College

Abstract: Information Security means protecting information and information systems from unauthorized access. Cryptography is used in Information Security to protect information through the technique named by encryption and decryption. The project is about the design of a new Cryptographic algorithm namely "Sea Encryption Algorithm (SEA)" for securing the information. It consists of two phases namely encryption and decryption separately. In the encryption module, it accepts the actual text (A) and key (K) for encryption and it divide both the actual text and key in different process. The decryption can be done by using the code sheet, which includes three types of code namely the Accept code, Print code and the Input code. The decrypted data can be viewed by the receiver if the person knows the key and the code sheet design. It provides less time complexity and overcomes the disadvantages of existing systems like AES, DES and DDES.

Keywords: Sea. Encryption, code, sheet

I. INTRODUCTION

The algorithm is designed in such a way that it breaks the attacks existed on AES, DES. Encryption and Decryption process can be done by the sender and the receiver. It provides large amount of security and confidentiality. The time complexity is comparatively low to the existing systems. The designed application is to motivate a large number of people because it is User Friendly, Highly Secured, Possessing technical and operational feasibility.

Information security is a broader term than IT Security or Internet Security or Enterprise Data Security. It looks at protecting / safeguarding information system from anyone including employees, consultants, supplies, customers and of course malicious hackers. Some of the specialty areas within security are Network security, Security testing, Information systems auditing. Cryptography is the science of information security [1]. It includes techniques such as microdots, merging words with images, and other ways to hide information in storage or transit. Cryptography is most often associated with scrambling plain text into cipher text. This process is termed as encryption. The reverse process of encryption is termed as decryption.

The proposed algorithm is named as SenthilAnanth Kumar (SeA) Encryption Algorithm (SeA). The main domain of the algorithm is for information security. The algorithm satisfies all the four objectives of cryptography. They are,

(a). Confidentiality
(b). Integrity
(c). Non-repudiation
(d). Authentication

The process of sea encryption algorithm is to accepts the actual text (A) and key (K) for encryption and it divide both the actual text and key in different process. The process, P is defined by it will do the process one by one. Here each process having four phases and each phase having ten steps. During the phases, the values are passed to four tables namely, Table-I, Table-II, Table-III and Table-IV and each table consists of 16 shuffled hexadecimal values. Especially the process defined based on the following three categories:

$$\boxed{P = \{P1, P2, P3\ldots Pn\}}$$

If A > K then the process is based on A and defined by P1 then check the condition until A=K

If A < K then the process is based on K and defined by P2 then check the condition until A=K

If A = K then the Process (P) is based on both the P1 & P2.

The Code Sheet contains three types of codes. They are

(a). Input Code
(b). Print Code
(c). Accept Code

And it having 66 codes for the above three types including alphabets, numbers and special characters.

The maximum time complexity (T) of this algorithm is defined by,

$$\boxed{T = O\ (\log 2\ (A + K)) + C}$$

Where, C is constant. SEA has only 4 phases and each having 10 steps. For (log 2 (A + K)), the comparisons made between the K and A based on the two conditions one is (K > A) and another one is (K < A).

If both the two conditions (mentioned above) are involved for encryption then the time complexity (T) is,

$$\boxed{T = O\ (\log 2\ (A + K))}$$

$$\boxed{T = O\ (\log 2\ (A)) + C.}$$

Suppose the comparisons are only based on the key (K) then

$$\boxed{T = O\ (\log 2\ (K)) + C.}$$

II. PROBLEM STATEMENT

The existing standard algorithms are faced with many problems such as Security attacks, Less Confidentiality, Less Key Strength and High Overhead. The Scope of the project is The SeA Encryption Application is a standalone application that can be typically installed on the sender and receiver systems. The algorithm is simple to understand. The key size range is 1016 bits. Lower overhead affords flexibility. Hardware and Software suitability and less memory space.

III. LITERATURE SURVEY

A. Advanced Encryption Algorithm (AES):

Originally known as Rijndael after its Belgium creators Daemen-Rijmen. Endorsed as AES by the US National Institute of Standards and Technology (NIST) in 2002. Suitable for a wide variety of platforms - ranging from smart cards to servers. Much simpler, faster and more secure.

AES is an iterative algorithm. Each iteration is known as Round. The number of rounds depends on key and data block size. Each round consists of four transformations: Sub Bytes, Shift Rows, Mix Columns and Add Round Key [2].

The standard comprises three block ciphers, AES-128,AES-192, AES-256.Each AES cipher has 128-bit block size with key sizes of 128,192 and 256 bits respectively.

a. Related-key Attack:

A related–key attack can break upto nine rounds of 256-bit AES.a chosen-plain text attack can break 8 rounds of 192-bit and 256 bit AES, and 7 rounds of 128-bit AES, although the work load is impractical at $2^{128\ -119.}$ [3]

B. Data Encryption Standard (DES):

It is based on a symmetric-key algorithm that uses a 56-bit key. the algorithm was initially contraversial with classified design elements, a relatively short key length and suspicious about a national Security Agency(NSA) backdoor [10].

a. Brute Force Attack:

DES is now consideredinsecure because a brute force attack is possible(EFF DES cracker). it requires 2^{43} known plain text and has a time complexity of $2^{39\text{-}43}$, under a chosen – plain text assumption, the data complexity can be reduced by a factor of four[4].

The drawbacks of the existing system are described below as follows:

a) The existing algorithms namely the AES,DES AND DDES are broken by several attacks namely AES,DES,and DDES.
b) The key size is very less.
c) It is profound to security attacks like brut force attack and reative key attack
d) It is not much simple to understand.
e) The algorithm is very difficult and tedious to perform if the key size increases.

IV. PROPOSED SYSTEM

The algorithm holds all the basic principles of information security and overcomes all the disadvantages of AES, DES, and DDES.

A. Strength Of Sea Algorithm:

a. For decryption, the algorithm id designed using Code Sheet for giving input. The Encrypted text (A) and the key (K) both are giving to the algorithm through Code Sheet only.
b. In Code Sheet 3 types of codes are available for 66 characters. So totally, 198 codes are there, from that the input code is framed by using ASCII codes that are used for giving input (type the input).
c. The other two types are used for displaying and accepting (converting) purposes. Therefore, the input given to the algorithm using Code Sheet is one of the advantages of the algorithm.
d. The next advantage is to increase the strength of the key (S) through the same algorithm.
e. Because providing the high strength of the key and strong encryption algorithm is a critical and challenging for increasing the difficulty of the attack.
f. The third one is ‘n’ number of comparisons based on the two conditions that are (i) A < S (ii) A > S. So the cipher text (C) is based on the strength of the key (S)
g. . So the intruder or cryptanalyst cannot guess the key or any parts of the actual text.

V. PROBLEM DEFINITION

The main aim of the algorithm is to increase the security level of the given information (actual text) based on the giving input and the increase the strength of the key through the number of comparisons. The comparisons are similar to the binary search method in encryption process. The decryption is designed to take encrypted text (A) and key (K) using Code Sheet.

A. Encryption:

In encryption phase, the sender preferred to encrypt the original data specifies the location of the file containing the original data. The sender then specifies the location of the file in which the desired encrypted data is to be saved.

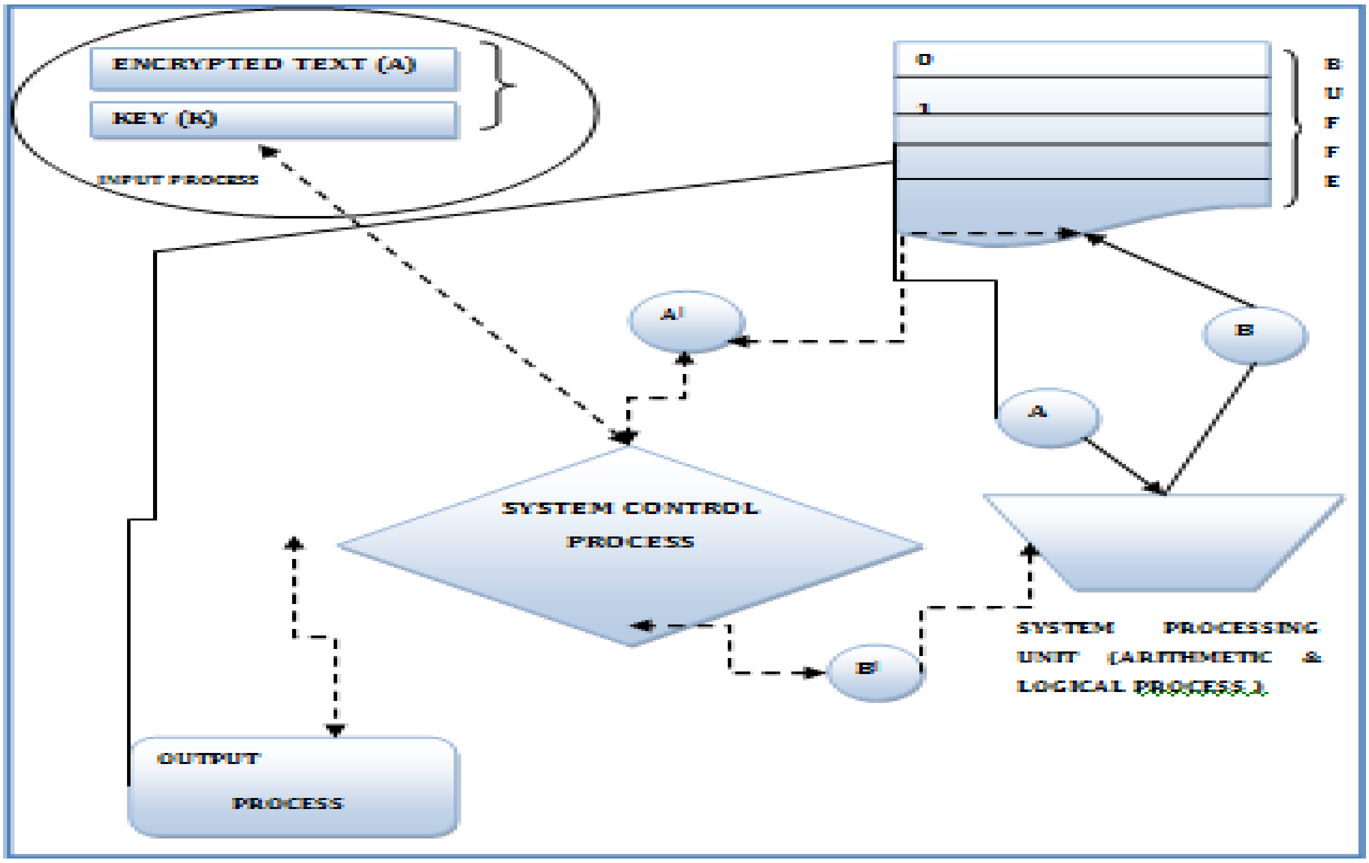


Figure.1 a & b – involved all tha mathematical process including the arithmetic and logical operations . The data is sent through a & b.a$^{|}$ & b $^{|}$- they are the control lines between the system process and the memory

B. *Decryption:*

In decryption phase, the receiver decrypts the sent encrypted data by using the code sheet and specifying the key. The receiver then can view the decrypted data in the specified location. In case of any abnormal activities during when the keyboard is locked, it assumes as interference of hackers and deletes the whole file by closing the entire application. The overall system architecture for the decryption process is illustrated in figure.

VI. MODULE DESCRIPTION

The project is totally divided into three modules,

MODULE 1- ENCRYPTION
MODULE 2-CODE SHEET DESIGN
MODULE 3-DECRYPTION

A. *Encryption:*

The encryption process in SeA algorithm uses uncomplicated methodology. The encryption methodology is as follows,

a. *Methodology:*

a. The encryption process at first accepts the Actual Text from the sender.
b. The process is set in such a way that once it has accepted the actual text it will start generating the corresponding ASCII values for all the characters mentioned in the actual text [5].
c. According to binary search method, The ASCII values are divided into two and separated as processes as illustrated below:

The process $P_1 = \{A_1, A_{n/2+1}\}$ is taken. First it will pass to the Position Table (mentioned below) that consists of alphabets and its shuffled values. The table contains 26 characters. Then the process continues which is similar to decryption process.

B. *Code Sheet Design:*

a. The Code Sheet is designed to accept the text through the respective numbers of each character when keyboard is locked.
b. The permutation and combination are applied on 66 characters on keyboard to design the Code Sheet Design [9].
c. In application, the Code Sheet consists of three types of code:
   a) Input code (IC),
   b) Print code (PC) and
   c) Accept code (AC).
d. The Code Sheet contains 66 characters for each category as follows.

For example,
The actual text (A) = “abc012………”

(a). ***Input Code-*** The input of each character is entered by pressing “ALT+along with its corresponding number “.

(b). ***Print Code-*** If the input for letter ‘a’ is given the corresponding another character will be printed on to the screen.

(c). ***Accept Code***- If the input for letter 'a' is given the memory will accept the letter 'a' whereas print another character on the monitor screen so that third person intrusion are avoided.

C. Decryption:

The SeA Encryption Algorithm will refer Code Sheet first then it will go for comparison of encrypted text (A) and key (K) and finally it will go for the process (P). It accepts the Encrypted text(a) and key(K) and defines the process as,

$A = \{ A_1, A_2, A_3, \ldots, A_n \}$

$K = \{ k_1, k_2, k_3, \ldots, k_n \}$

The process P is defined as,

$P = \{ P_1, P_2, P_3, \ldots, P_n \}$

The first step is increase the strength of the key (K) then compare A with K. after that three options are provided as

A is less than K (A<K)

A is greater than K (A>K)

A is equal to K(A=K)

This process is similar to the binary search method

The steps are defined in the following as:

i. If A > K then

The process is based on A and defined by P_1 then check the condition until A = K.

ii. If A < K then

The process is based on K and defined by P_2 then check the condition until A = K.

iii. If A =K then

The process (P) is based on both the P_1& P_2.

The overall process is defined in the following figure 2. (ii). When the algorithm meets the process A, then again it'll do the same process. So the cipher text (C) may have a single value or group of values, because C is based on the number of comparisons of A and K. The three cases are analyzed as,

CASE 1: A < K

The process (P) is based on the K. First it will divide K into two and it does the process between the two parts of K. then again compares it with A. suppose A< K again, it'll do the same process until A = K.

The sequence of the process based on K is illustrated in the following. Where the process,

$P_1 = \{K_1, K_{n/2+1}\}$, $P_2 = \{K_2, K_{n/2+2}\}$, $P_3 = \{K_3, K_{n/2+3}\}$

Table 1 code sheet design

ACCEPT	**a**	**B**	**c**	**…**	**0**	**1**	**2**	**...**	**9**	**@**	*****	**+**	**…**
PRINT	**~**	**8**	**R**	**…**	**D**	**:**	**&**	**....**	**^**	**q**	**v**	**t**	**…**
INPUT	**240**	**127**	**159**	**...**	**154**	**109**	**234**	**…**	**211**	**187**	**192**	**233**	**…**

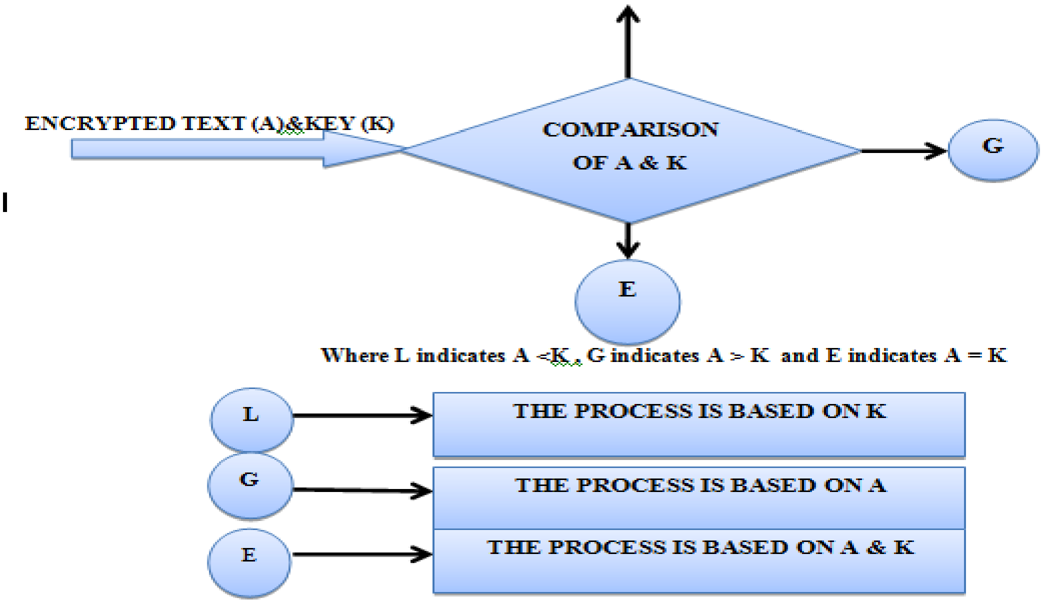

ENCRYPTED TEXT (A)&KEY (K)
COMPARISON OF A & K
G
E
I
Where L indicates A <K, G indicates A > K and E indicates A = K
L
THE PROCESS IS BASED ON K
G
THE PROCESS IS BASED ON A
E
THE PROCESS IS BASED ON A & K

Figure.2 Comparisons Of A & K

Case 1: A < K

The process (P) is based on the K. First it will divide K into two and it does the process between the two parts of K. then again compares it with A. suppose A< K again, it'll do the same process until A = K.

The sequence of the process based on K is illustrated in the following. Where the process,

$P_1 = \{K_1, K_{n/2+1}\}$, $P_2 = \{K_2, K_{n/2+2}\}$, $P_3 = \{K_3, K_{n/2+3}\}$

CASE 2: A > K

The process (P) is based on the A. First it will divide A into two and it does the process between the two parts of A. then again compares it with K.

Suppose A > K again, it'll do the same process until A = K.

The sequence of the process based on A is illustrated in the following. Where the process,

$P_1 = \{A_1, A_{n/2+1}\}$, $P_2 = \{A_2, A_{n/2+2}\}$, $P_3 = \{A_3, A_{n/2+3}\}$

The process from P_1 to P_n is over; then again it will compare with A (case 1) and/or with K (case 2) and again do the process based on the cases.

CASE 3: A =K

The algorithm first increases the strength of K and does the same process (P).The processes are:
$P_1 = \{A_1, K_2\}$, $P_2 = \{A_2, K_3\}$, $P_3 = \{A_3, K_4\}$ …

D. Description Of The Process (P_1) For Both Encryption And Decryption Process:

a. In the Encryption process, the ASCII value of the characters are divided into two by Binary Search Method and each defined process are taken and distributed among the tables as explained below [6].

b. In the Decryption process, it compares the Encrypted text (A) and Key (K) based on the three conditions. Each defined process are taken and distributed among the tables as explained below.

c. The process $P_1 = \{A_1, K_2\}$;

d. First it will pass to the Position Table (mentioned below) that consists of alphabets and its shuffled values. The table contains 26 characters.

This is illustrated in position table as below

Table 2(i) Position Table 1

A	B	C	D	E	F	G	H	I
13	16	2	6	25	12	19	23	3
J	K	L	M	N	O	P	Q	R
9	5	20	15	1	22	11	18	10
S	T	U	V	W	X	Y	Z	
8	17	24	4	26	7	21	14	

e. P_1 is passed to the Position Table and the relevant value, V is defined as,

$\mathbf{V_1 = \{ V_n , V_m \}}$.Next, determine the equivalent four digit binary value (B) and make it four parts. The B is defined by, $\mathbf{B = \{ BV_1,BV_2,BV_3,BV_4 \}}$

The value of B_1 is pass to the Phase-I. Before discuss the four phases here we defined the general steps. They are as follows:

E. Steps of Sea for Process (p):

There are 4 phases as phase-I, phase-II, phase-III, phase-IV. First, the B value is passed to phase-I and then to phase-II, phase-III, phase-IV. Each phase consists of ten steps to be carried out. The ten steps carried out during when the B value passed to phase-I is explained below [7][8],

a. Interchange the B values

b. Split the B values.

After interchange, the values divided into two parts for Phase-I, four parts for Phase-II, eight parts for Phase-III and sixteen parts for Phase-IV.

c. Merge the values and make it two parts.
For example: $BV_1\ BV_2 \ \ | \ \ BV_3\ BV_4$

d. The values are pass to the Table-I and replace the relevant values.

The table-I having sixteen shuffled hexadecimal values. The table-I is as follows:

Table 3 (ii) position Table 2

0	1	2	3	4	5	6	7
3	5	C	8	B	E	0	4
8	9	A	B	C	D	E	F
A	7	F	D	1	6	2	9

e. Shift the bits.

Shift the bits between the parts. For example if the parts are defined by n then, shifts (n+ (n-1)) times.

f. Pass it to the Table-II and replace the relevant values.

The table-II having sixteen shuffled hexadecimal values. The table-II is as follows:

g. Determine the ones complement of values.
Add 1 to the B values.

Table 4. (iii) Position table 3

0	1	2	3	4	5	6	7
4	7	E	6	A	D	9	C
8	9	A	B	C	D	E	F
B	F	2	8	5	3	8	1

h. Pass it to the Table-III and replace the relevant value.

The table-III having sixteen shuffled hexadecimal values. The table-III is as follows:

Table 5 (iv) Position Table 4

0	1	2	3	4	5	6	7
7	C	A	F	2	1	4	B
8	9	A	B	C	D	E	F
E	3	5	6	8	9	0	D

i. Convert all zeros are ones and ones are zeros.

j. Pass it to the Table-IV and replace the relevant value.

The table-IV having sixteen shuffled hexadecimal values. The table-IV is as follows:

Table 6 (v) Position Table 5

0	1	2	3	4	5	6	7
B	9	F	5	C	A	2	E
8	9	A	B	C	D	E	F
0	D	7	1	3	4	6	8

Finally merge all the bits.

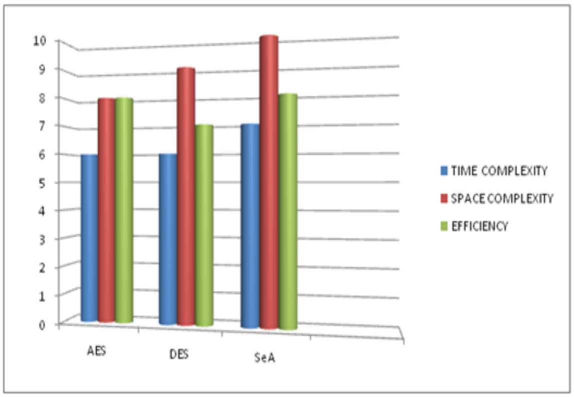


Figure :7.4 SeA Versus AES, DES

VII. CONCLUSION

The features of SeA Encryption Algorithm (SEA) and its further enhancements are concluded. Protecting confidential information is a business requirement, and in many cases also an ethical and legal requirement. For the individual, information security has a significant effect on privacy, which is viewed very differently in different cultures. The encryption methods must provide the confidentiality, integrity and availability of information. The algorithm is concluded as,

a. The existing encryption systems may secure the data or information or text but it has less strength of the key. Whatever the strong algorithm may develop for encrypting the text or data the strength of the key must be strong and high. SeA Encryption Algorithm having both strong algorithm and high key strength.

b. SEA having 'n' comparisons and it based on both the actual text and strength of the key. First the key is encrypted then compare with actual text and the comparisons based on the two conditions, they are (i) A > S and (ii) A < S. So here nobody can guess the 'n' number of comparisons.

c. One more special feature of this algorithm is Code Sheet because whatever the input can give using it only. The algorithm gets the correct input only through the Code Sheet.

VIII. FUTURE ENHANCEMENT

a. The algorithm is designed for only text (character). This can be improved and applied to images.

b. On further the SeA Encryption Algorithm can be improved with constant cipher text that means whatever the size of the actual text and key, after encryption the cipher text is a single value. So, the number of comparisons and processes can be increased.

c. This can be further applicable for network security by making improvements and include the mobile applications like SMS, MMS and etc.

d. The manpower involved during when the keyboard is locked by looking into the code sheet and entering the characters will be reduced in future.

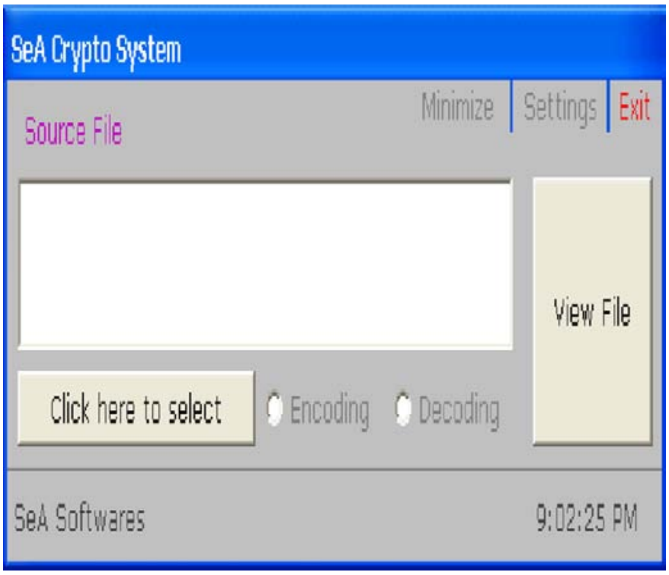
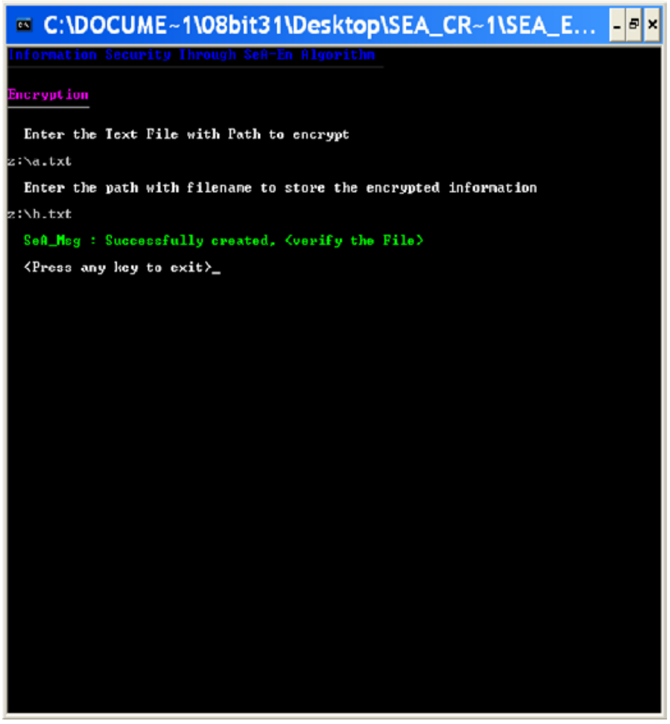


Figure 3.Sea Application Window

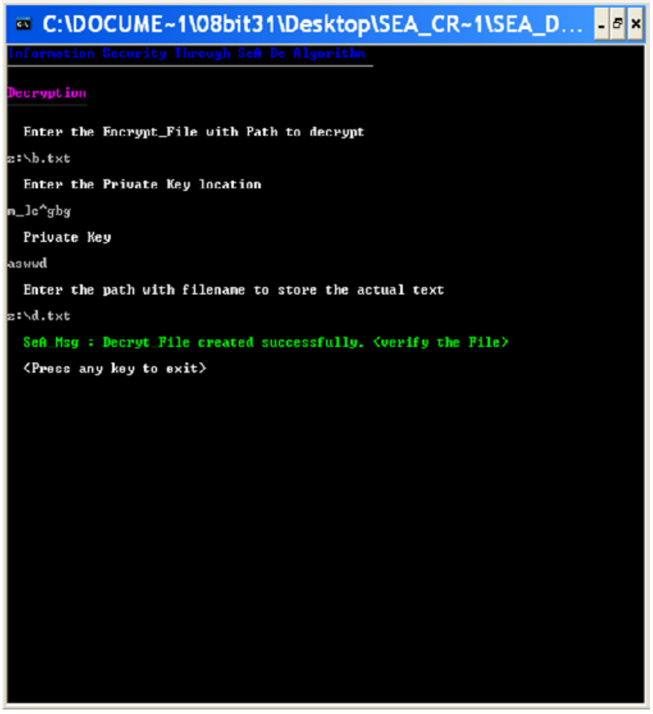


```
C:\DOCUME~1\08bit31\Desktop\SEA_CR~1\SEA_E...
Information Security Through SeA-En Algorithm

Encryption

  Enter the Text File with Path to encrypt
z:\a.txt
  Enter the path with filename to store the encrypted information
z:\h.txt
  SeA_Msg : Successfully created. <verify the File>
  <Press any key to exit>_
```

Figure 4. Encryption window

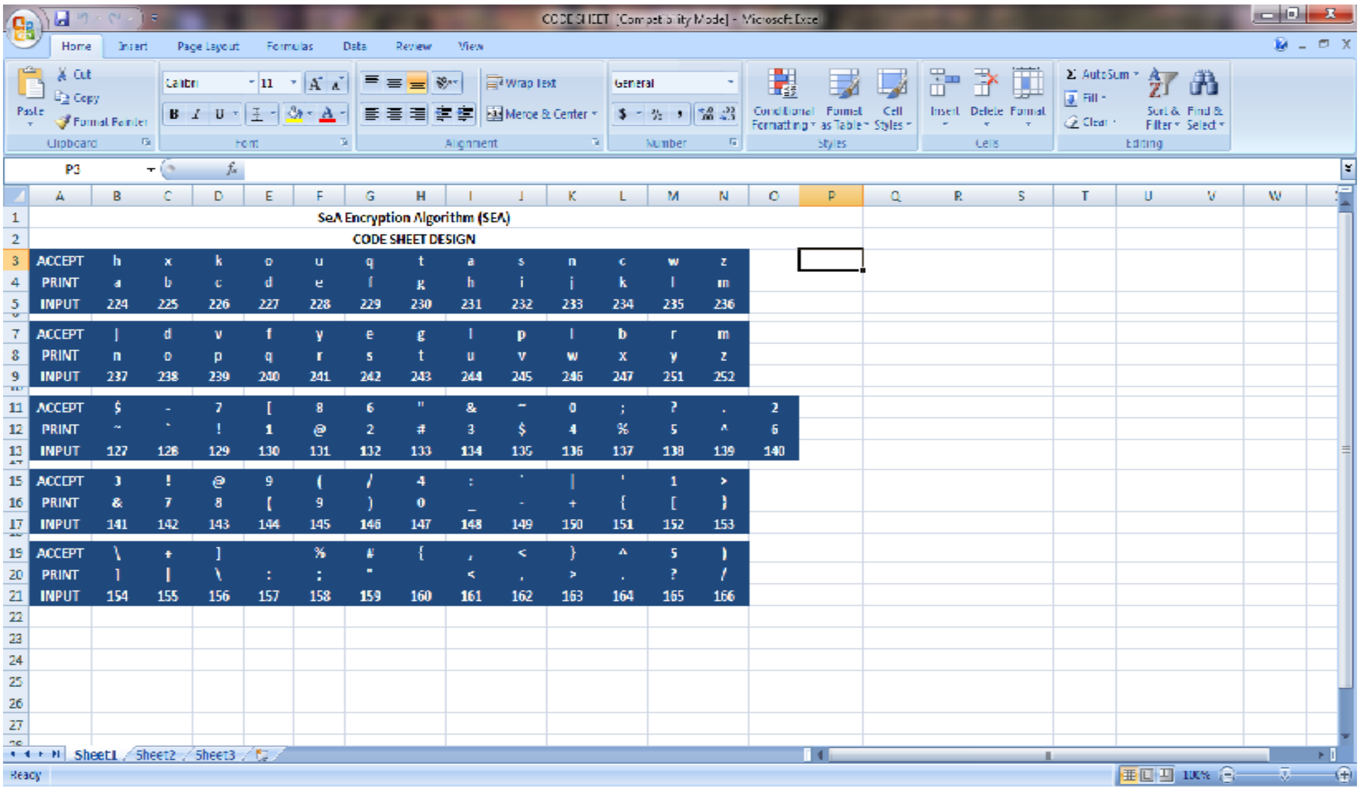


```
C:\DOCUME~1\08bit31\Desktop\SEA_CR~1\SEA_D...
Information Security Through SeA De Algorithm

Decryption

  Enter the Encrypt_File with Path to decrypt
z:\b.txt
  Enter the Private Key location
n_Jc^gbg
  Private Key
aswwd
  Enter the path with filename to store the actual text
z:\d.txt
  SeA Msg : Decryt File created successfully. <verify the File>
  <Press any key to exit>
```

Figure 5. Decryption window



SeA Encryption Algorithm (SEA)

CODE SHEET DESIGN

ACCEPT	h	x	k	o	u	q	t	a	s	n	c	w	z
PRINT	a	b	c	d	e	f	g	h	i	j	k	l	m
INPUT	224	225	226	227	228	229	230	231	232	233	234	235	236
ACCEPT	j	d	v	f	y	e	g	l	p	l	b	r	m
PRINT	n	o	p	q	r	s	t	u	v	w	x	y	z
INPUT	237	238	239	240	241	242	243	244	245	246	247	251	252
ACCEPT	$	-	7	[	8	6	"	&	~	0	;	?	.	2
PRINT	~	`	!	1	@	2	#	3	$	4	%	5	^	6
INPUT	127	128	129	130	131	132	133	134	135	136	137	138	139	140
ACCEPT	3	!	@	9	(	/	4	:	`	|	'	1	>
PRINT	&	7	8	(	9	)	0	_	-	+	{	[	}
INPUT	141	142	143	144	145	146	147	148	149	150	151	152	153
ACCEPT	\	+	]		%	#	{	,	<	}	^	5	)
PRINT	]	|	\	:	;	"		<	,	>	.	?	/
INPUT	154	155	156	157	158	159	160	161	162	163	164	165	166

Figure.6 Code Sheet Design

IX. REFERENCES

[1]. Chien Hung-Yu (2008). “The Computer Journal, Volume 51 Issue 4 (July 2008), pp.419-434.ISSN: 0010-4620”.

[2]. Kuo Chin-Fu, Pang Ai-Chun, Chan Sheng-Kun (2009). “IEEE Transactions on Parallel and Distributed Systems”, Volume 20 Issue 1(January 2009), pp.48-58. ISSN: 1045-9219”.

[3]. Stallings William (2006). “Cryptography and Network Security- Principles and Practices (4th Ed.)(2006), pp.72-86,134-165.ISBN 978-81-203-3018-4.

[4]. Miyali Atsuko (2007). “ICISC'07 Proceedings of the 10th international conference on Information security and cryptology (2007), pp.282-296. ISBN: 3-540-76787-8 978-3-540-76787-9”.

[5]. Nasako Takashi, Murakami Yasuyuki, Kasahara Masao (2008). “IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, Volume E91-A Issue 10 (October 2008), pp.2833-2842. ISSN: 0916-8508”.

[6]. Shu Tao, Krunz Marwan, Liu Sisi (2010). “IEEE transactions on Mobile Computing, Volume 9 Issue 7 (July 2010), pp.941-954. ISSN: 1536-1233”.

[7]. Layton, Timothy P, (2007). “Information Security: Design Implementation, Measurement, and Compliance. Auerbach Publication (2007)”. ISBN 978-0-8493-7087-

[8]. Harris, Shon (2008).” All-in-one CISSP Certification Exam Guide (4th Ed.). New York, McGraw-Hill (2008)”. ISBN 978-0-07-149786-2.

[9]. Dhillon, Gurpreet (2007). “Principles of Information Systems Security: text and cases. John Wiley & Sons (2007)”. ISBN 978-0471450566.

[10]. Schneier, Brush (1996). “Applied Cryptography.New York: Wiley (1996)” p.229.ISBN 0471128457.