Volume: 07 Issue: 02 Pages: 2694-2699 (2015) ISSN: 0975-0290

MULTI-STAGE ENCRYPTION USING SEEDED SDES

Dr.S.Kiran
Asst. Prof Department of Computer Science and Engineering, YSREC of Y V University, Proddatur
Email: rkirans125@gmail.com
R. Pradeep Kumar Reddy
Asst. Prof Department of Computer Science and Engineering, YSREC of Y V University, Proddatur
Email: pradeepmadhavi@gmail.com
J.Venkata Sivajaya Sree
Department of Computer Science and Engineering, YSREC of Y V University, Proddatur
Email: j.v.s.jayasree@gmail.com
D.Naga Sravanthi
Department of Computer Science and Engineering, YSREC of Y V University, Proddatur
Email: d.nsravanthi2010@gmail.com

----------**ABSTRACT**----------
Now-a-days the usage of internet increases tremendously so, there is a need of security for the data. Cryptography is a process of scrambling the data into unknown format which provides security to the data. Modern cryptography is mainly based on mathematical theory and computer science practice. Cryptography process is done with the help of encryption and decryption. The basic two ideas behind the cryptography technique are substitution and transposition. This paper presents a multistage encryption algorithm. At the end of each stage an intermediate cipher is produced. The key is generated by using SEEDED SDES algorithm. Final cipher text is derived from the local binary pattern (LBP).

Keywords - D**ecryption, Encryption, Railference, SEEDED SDES key generation, Substitution, Transposition.**

Date of Submission: July 31, 2015 Date of Acceptance: Sep 09, 2015

1. INTRODUCTION

Cryptography is the practice and study of techniques for secure communication in the presence of third parties. Cryptography means, a method of transmitting data in sandwiched between a two persons, i.e. those (sender) for whom (receiver) can only read and process the data. A message in its original format, readable by an attacker is plaintext[1] .A message is changed to be unreadable format by sender to anyone except the intended recipient is cipher text. The term is most often associated with encryption and decryption. The scrambling of original text (plain text) into cipher text is known as encryption, and then back again is known as decryption.

The main traditional cipher types are transposition ciphers and substitution ciphers. A transposition cipher is one, which rearranges the order of letters in a message. For example ‘computers’ becomes ‘pmocusret’. The cipher, which systematically replaces letters or groups of letters with other letters or group of letters, is referred as substitution cipher. For example: ’talk less work more’ becomes ‘ubml mftt npsf’. An early substitution cipher was the caeser cipher, in which each letter in the plaintext was replaced by a letter with some fixed number of positions further down the alphabet[2]. Application of cryptography includes ATM cards, computer passwords and electronic commerce.

In the 20th century, cryptography was predominantly concerned with linguistic (scientific study of language) and lexicographic patterns (greedily generated error-correction codes). Then the emphasis has shifted, and cryptography now makes extensive use of mathematics, including aspects of information theory (branch of applied mathematics, electrical engineering and computer science), computational complexity(theory of computation), statistics, combinatory(countable discrete structures), abstract algebra, number theory(pure mathematics) and finite mathematics generally[3].

1.1. Background

The word cryptography is derived from the Greek language ‘kryptos’ means “hidden” or “secret”.

At 2000bc cryptography was origined with the egyptian practice of hieroglyphics, which consist of complex pictograms. The first known use of a modern cipher was by julius Caesar. Julius Caesar created a system in which each character in his message was replaced by a character three positions ahead of it in the roman alphabet, why because he did not trust his messengers when communicating with his governors and officers.

The cryptosystem services are data confidential, data integrity, authentication and non-repudiation. Data

Volume: 07 Issue: 02 Pages: 2694-2699 (2015) ISSN: 0975-0290

Confidentiality is a set of rules, which imposes access limits and restrictions on the information. The main aim of Data integrity is to prevent unintentional changes to information and the control of protecting data from unauthorized parties. Authentication performs the conformation of truth attribute of a single piece of data or entity.

Now a days cryptography has crooked into a battleground of the world's best mathematics and computer scientists. The ability to securely store and transfer sensitive information has proved a critical factor in success in war and business[3].

1.2 Types of cryptography

1.2.1 Symmetric key cryptography

In the simpler types of cryptography, the same key is used to encrypt and decrypt the data. Some of the symmetric algorithms are DES, 3DES, AES, IDES, RC4, RC5.

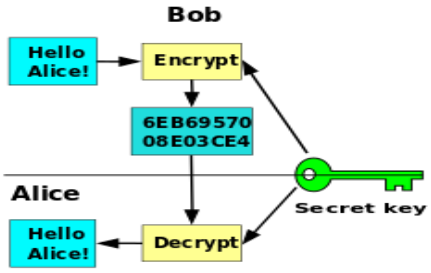


Fig 1.1: Symmetric key cryptography.

1.2.2 Asymmetric key cryptography

In this type of cryptography, the encryption is done by one key and the decryption is done by another key .one of this key is private key and the another key is public key (known to everyone).

Some of the asymmetric algorithms are RSA, ECC (Elliptical curve Cryptography), Elgamal. These systems use two keys, a public key known to everyone and a private key that only the recipient of messages uses.

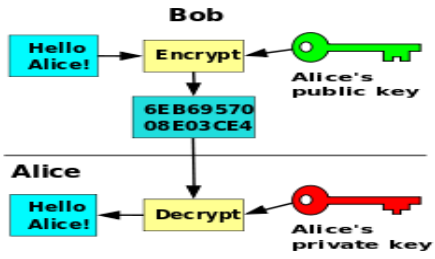


Fig 1.2: Asymmetric key cryptography

1.3 Existing work

The SDES key generation is done by using permutation method. Two keys are generated from the SDES key generation algorithm .Among them, select the smallest one as the key.

1.3.1 Encryption Algorithm

Existing Encryption algorithm is done in three steps.caesar cipher substitution, transposition and arithmetic and logical operations are applied to generate cipher text. The three steps are as follows:

Step 1: An automatic key is generated through the existing SDES key generation algorithm[4]. In the first round, caesar cipher substitution[5] is performed with the help of private key produces an intermediate cipher 1.
Step 2: Apply crossover to the intermediate cipher 1, to transpose the character's position, mutation process is involved. At the end of round 2 an intermediate cipher 2 is produced.
Step 3: Round 3 encompasses all the arithmetic and logical operations to obtain a final cipher text.

1.3.2 Decryption Algorithm

Decryption algorithm is reverse process of an encryption algorithm. The three decryption steps are as follows:

Step 1: Take the final cipher text and perform all basic Arithmetic and logic operations to it. It produces the intermediate plaintext 1.
Step 2: Apply crossover process to the intermediate Plaintext1 followed by the mutation technique which gives the intermediate plaintext2.
Step 3: Finally, reverse caesar cipher substitution is Involved using private key as declared in the encryption algorithm.

2. PROPOSED WORK

The proposed algorithm uses seeded sdes key generation, railference and local binary pattern provides more complexity for the text. The advantage of high complexity, the unauthorized person face very difficult to understand the original plain text.

2.1 SEEDED SDES Key generation

2.1.1 Algorithm steps

Step 1: Initially generate random 64 binary bit sequence.
Step 2: Divide those 64 bits into 8 chunks, each chunk consists of 8 bits.
Step 3: Retrieve MSB bit from left to right of each chunk, which results 8 bit sequence.
Step 4: Compute the decimal number to the above 8 bit Sequence that is referred to be as key.

Volume: 07 Issue: 02 Pages: 2694-2699 (2015) ISSN: 0975-0290

2.1.2 Flow chart for SEEDED SDES key generation

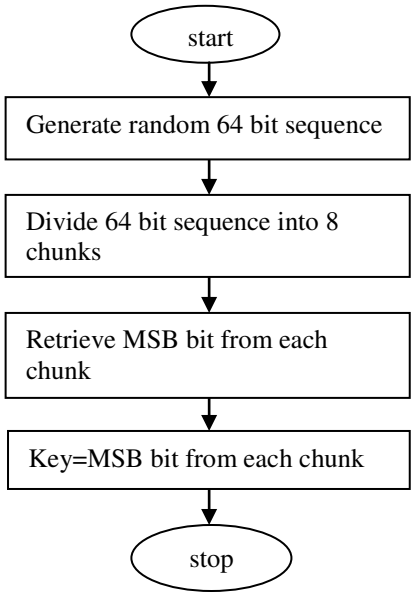


Fig 2.1: seeded sdes key generation

2.1.3 Example for SEEDED SDES key generation

Step 1: 64 bit sequence is
11010110010101011100110011110000011101 1
1100100110011101011000110
Step 2: Divide this sequence into 8 chunks:
11010110 | 01010101 | 11001100 | 11110000 |
01110111 | 10010011 | 00111010 | 11000110
Step 3: Retrieve most significant bit from each chunk, then the production of key in binary is 10110101.
Step 4: The decimal value for the key is 181.

2.2. Encryption Algorithm

By using the key, generated from seeded sdes algorithm and substitution method an intermediate cipher is generated. Apply railferance technique on intermediate cipher and produce intermediate cipher text 2.Combination of arithmetic and logical operations are applied on intermediate cipher 2 and produces the final cipher text.

2.2.1 Algorithm steps

Step 1: An intermediate cipher 1 is produced by using caesar cipher substitution method with the help of private key [5]. Privates key is obtained from SEEDED SDES key algorithm.
Step 2: Perform the railference technique for the Intermediate cipher 1,inverse of text is involved. An intermediate cipher text 2 is produced.
Step 3: The fina l cipher text is obtained by using local binary pattern[7]. The process of local binary pattern is to place the 0^{th} position bit into 3^{rd} position bit, the remaining bits (previously 1^{st}, 2^{nd} and 3^{rd} position bits) are moved forward from left to right side. At the final stage, it encompasses all arithmetic, logical operations and local binary pattern technique yields final cipher text.

Table: LBP Diagram:

2^0	2^7	2^6
2^1		2^5
2^2	2^3	2^4

Conditions:

For i<j: 2^7 2^6 2^5
i>j: 2^3 2^2 2^1
i=j 2^4 2^0

after LBP text is: i<j i=j i>j

2.2.2 Flowchart for proposed encryption algorithm

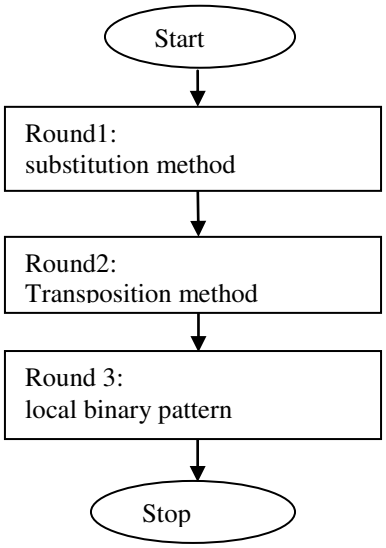


Fig 2.2.1: Encryption algorithm

Table 1: substitution method lookup table

Character	Value	Character	Value
!	0	R	49
“	1	S	50
#	2	T	51
$	3	U	52
%	4	V	53
&	5	W	54
‘	6	X	55
(	7	Y	56
)	8	Z	57
*	9	[	58
+	10	\	59
‘	11	]	60
-	12	^	61
.	13	_	62

Volume: 07 Issue: 02 Pages: 2694-2699 (2015) ISSN: 0975-0290

/	14	`	63
0	15	a	64
1	16	b	65
2	17	c	66
3	18	d	67
4	19	e	68
5	20	f	69
6	21	g	70
7	22	h	71
8	23	i	72
9	24	j	73
:	25	k	74
;	26	l	75
<	27	m	76
=	28	n	77
>	29	o	78
?	30	p	79
@	31	q	80
A	32	r	81
B	33	s	82
C	34	t	83
D	35	u	84
E	36	v	85
F	37	w	86
G	38	x	87
H	39	y	88
I	40	z	89
J	41	{	90
K	42	|	91
L	43	}	92
M	44	~	93
N	45		
O	46		
P	47		
Q	48		

2.2.3 Example for Encryption algorithm

Round 1
Plaintext=computer
key=181

Table 2: Result of Round1

plaintext(p)	Corresponding value(v)	C=(v+key)%94	Corresponding character of C
c	66	59	\
o	78	71	h
m	76	69	f
p	79	72	i
u	84	77	n
t	83	76	m
e	68	61	^
r	81	74	k

Intermediate cipher1 is **\hfinm^k**

Round 2 Railference
Write intermediate cipher 1 as follows:
\ → f → n → ^
h → i → m → k
string1=\fn^
string2=himk
string=string1+string2
string=\fn^himk
IC2=inverse(string)
Intermediate cipher2(IC2)=**kmih^nf**

Round 3
Calculate binary equivalent for each character in IC2.

Table 3: Combination of Arithmetic and Logic Operations

Intermediate cipher 2	Corresponding value	Equivalent binary	Reverse
k	74	01001010	01010010
m	76	01001100	00110010
i	72	01001000	00010010
h	71	01000111	11100010
^	61	00111101	10111100
n	77	01001101	10110010
f	69	01000101	10100010
\	59	00111011	11011100

Table 4: Local Binary Pattern

Reverse	Local binary pattern	Equivalent decimal value	ASCII character
01010010	01010001	81	Q
00110010	00110001	49	1
00010010	00010001	17	◄
11100010	11100001	225	ß
10111100	10110110	182	╢
10110010	10110001	177	▒
10100010	10100001	161	í
11011100	11010110	214	∏

Final cipher text is: **Q1◄ß╢▒ í∏**

2.3 Decryption Algorithm

The process of unlocking encryption information using cryptography is known as decryption.Local binary pattern,arithmetic and logical operations ,railference technique and substitution methods are applied on final cipher text and produces the original plain text.

2.3.1 Algorithm steps

Step 1: The final cipher text is decrypted by using all basic arithmetic, logical and Local Binary Pattern technique to produce the intermediate plaintext1.
The process of Local binary pattern is to place the 3rd position bit into 0th position bit and the previously 2nd, 1st ,0th bits are moved to 3rd, 2nd, 1st bit positions respectively.

Volume: 07 Issue: 02 Pages: 2694-2699 (2015) ISSN: 0975-0290

Step 2: Apply mutation of the intermediate plaintext1, railference technique for the plaintext. An intermediate plaintext 2 is produced.
Step 3: At the end of decryption algorithm, original plaintext is obtained with the help of all basic arithmetic, logical operations and Caesar cipher substitution method.

2.3.2 Flow chart for proposed decryption algorithm

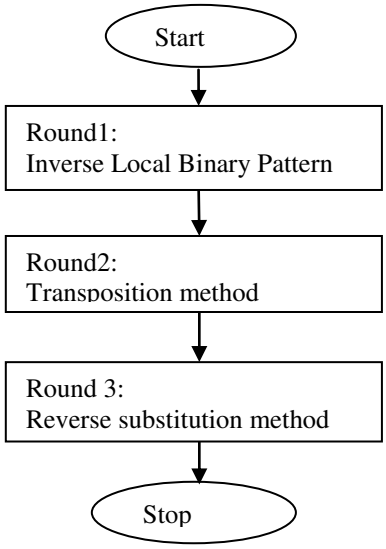


Fig 2.2.1: Decryption algorithm

2.3.3 Example for decryption algorithm:

Round 1:

Cipher text=:**Q1◄ß┤▒ í∏**

Table 5: Inverse Local Binary Pattern

Cipher text	Equivalent decimal value	Equivalent binary	Local binary pattern
Q	81	01010001	01010010
1	49	00110001	00110010
◄	17	00010001	00010010
ß	225	11100001	11100010
┤	182	10110110	10111100
▒	177	10110001	10110010
í	161	10100001	10100010
∏	214	11010110	11011100

Table 6: Combination of Arithmetic and Logic Operations

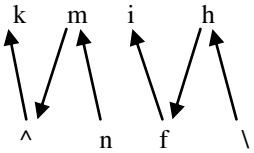
Local binary pattern	Reverse	Corresponding decimal Value	Corresponding character
01010010	01001010	74	k
00110010	01001100	76	m
00010010	01001000	72	i
11100010	01000111	71	h
10111100	00111101	61	^
10110010	01001101	77	n
10100010	01000101	69	f
11011100	00111011	59	\

Intermediate plaintext1 is **kmih^nf**
Round 2

I=inv(intermediate plaintext1)

I=\fn^himk

Railference



string1=\hfi
string2= nm^k
string=string1+string2
string=\hfinm^k
Intermediate plaintext2 is**:\hfinm^k**

Round 3
if((V+n)>key) then P=((V+n)%key)
else if((V+n+n)>key) then P=((V+n+n)%key)
else P=((V+n+n+n)%key)

Table 7: Reverse Substitution Method

Intermediate plaintext2	Corresponding numeric value(V)	P=(V+n)% key	Equivalent char
\	59	66	c
h	71	78	o
f	69	76	m
i	72	79	p
n	77	84	u
m	76	83	t
^	61	68	e
k	74	81	r

At the end of decryption, original plaintext is: **computer**

Volume: 07 Issue: 02 Pages: 2694-2699 (2015) ISSN: 0975-0290

3. ADVANTAGES

1. The key is generated through random number generation with 64 bit sequence.
2. The railference and local binary pattern methods give complexity to the intermediate cipher text.
3. High processing speed.

4. CONCLUSION

Security plays a vital role in communication channels, best example is internet. Now-a- days, billions of the people are using internet. Internet carries a huge amount of information such as mails, documents, sharing of files, business deals and so on. In order to protect the information from unauthorized persons, one needs better security mechanisms. For protecting information, most popular approach is cryptography. Cryptography is the art of secret writing. The main aim of cryptography is to see that the intended receiver can only understand the message. The proposed algorithm uses local binary pattern, railference, substitution method and seeded S-DES key generation. In the future work, this algorithm will be extended to use the UNICODE system support.

REFERENCES

[1] Govind Prasad Arya,Aayushi Nautiyal,ashishPant,Shiv Singh & Tishi Handa,"*A cipher design with automatic key generation using the combination of substitution and transposition techniques and basic arithmetic and logic operations*," the SIJ Transactions on computer science engineering & its applications

[2] S.G.Srikantaswamy and Dr.H.D.phaneendra,"*A cipher design using the combined effect of arithmetic and logic operations with substitutions and transposition techniques* , " International Journal of Computer Applications(0975-8887),vol.29,no.8,pp.34-36

[3] Jonathan Katz and Yehuda Lindell, Introduction to modern cryptography, Chapman and hall/CRC, Taylor and Francis group, 2008.

[4] S.Devi, Dr.V.Palanisamy, "*Multi-Level Encryption using SDES key generation with Genetic Algorithm*", international journal of engineering and computer science (IJECS) , vol.3 , issue.8 , page no: 7596-7576, aug 2014.

[5] B.Bazith Mohammed, "*automatic key generation of Caesar cipher*", international journal of engineering trends and technology (IJETT), vol.6,no.6,pp.337-339,dec.2013.

[6] S.G.Srikantaswamy and Dr.H.D.Phaneendra,*Improved Caesar cipher with random number Generation technique and multistage encryption*", International Journal on Cryptography and information+Security(IJCIS),vol2,no.4,pp.39-49,Dec.2012

[7] Di Huang,Caifeng Shin and Mohsen Ardabilian *"Local Binary Patterns and Its Application to Facial Image Analysis: survey"*, IEEE transactions on systems, man,and cybernetics_ part c: applications and reviews, vol.41,no.6,nov 2011.

Authors Profile

Dr.S.Kiran is Assistant Professor in the department of Computer Science and Engineering at Yogivenama University , Proddatur. He acquired M.Tech Degree from Nagarjuna University, Guntur. He completed Ph.D in computer science from S.K.University. He has been continuously imparting his knowledge to several students in research activities. He published many articles National and International journals. His research areas are image Processing, Cryptography and Network Security, Software Engineering and Data mining and Data ware house.

R. Pradeep Kumar Reddy is working as Assistant Professor in Department of CSE at Y.S.R Engineering College of Yogi Vemana University, Proddatur. He received his B.Tech degree in CSE from Bellary Engineering College, Bellary (VTU). M. Tech degree in CSE from S.R.M University, Chennai. He worked as Assistant Professor and Head of the department CSE, IT and MCA in Vaagdevi Institute of Technology and Science, Proddatur during the period 2005 to 2008. Later he joined as Assistant Professor and Head of the Department IT in Chaitanya Bharathi Institute of Technology and Science, Proddatur, during the period 2008 to 2009. He published many research articles in various National and International Journals. He attended National and International Conferences. He is pursuing PhD in digital image processing at Yogi Vemana University, Kadapa.

J Venkata Sivajaya Sree is a student in the department of Computer Science and Engineering at Y.S.R Engineering College of Y.V.U, Proddatur . She is studying 4th B.Tech in CSE. She attended many workshops and Seminars.

D Naga Sravanthi is a student in the department of Computer Science and Engineering at Y.S.R Engineering College of Y.V.U, Proddatur . She is studying 4th B.Tech in CSE. She attended many workshops and Seminars.