International Journal of Communication Networks and Security

Volume 1 | Issue 1 Article 3

2011

Computing Symmetric Block Cipher Using Linear Algebraic Equation.

Pradeep Kumar Mallick
C.V.Raman College of Engineering and Technology, pradeepmallick842@gmail.com

N.K. kamila
C.V.Raman College of Engineering and Technology, nkamila@yahoo.com

S. Patnaik
Interscience Institute of Management and Technology, srikantapatnaik@hotmail.com

Computing Symmetric Block Cipher Using Linear Algebraic Equation.

Pradeep Kumar Mallick[1], N.K.kamila[2], S.Patnaik[3]
[1,2] C.V.Raman College of Engineering and Technology
[3] Interscience Institute of Management and Technology
pradeepmallick842gmail.com[1], nkamila@yahoo.com[2], srikantapatnaik@hotmail.com[3]

Abstract: ***In this paper, a pair of symmetric block ciphers has been developed for encryption and decryption of text file. The characters in the file are represented by the ASCII codes. A substitution table and a reverse substitution table are formed by using a key. The process of encryption and decryption is carried by using linear algebraic equations. However, the cryptanalysis has been discussed for establishing the strength of the algorithm. Result and analysis exhibits that the current algorithm works well and more secured to break the cipher.***

Keywords: *ASCII codes, Encryption, Decryption, Substitution table.*

1. INTRODUCTION

In the present era of Information Technology, transmission of information in a secured manner is the primary concern of all agencies. Security is highly essential as intruders are very keen to rob the information with all their might and intelligence. Though several algorithms are very well developed in the literature [1-8]; it needs more technologies and algorithms to enrich the field of cryptography.

In this paper a text file in English language has been considered and represented each character is represented in its ASCII code. The set of characters are divided into blocks. A key K_0 has been selected basing upon the number associated with the blocks. Also introduced another key K being so that it modifies the cipher text in an appropriate manner. The encryption and decryption are carried out by using both K_0 and K.

The rest of the paper is organized as follows:
Section 2 analyses the problem and develops a substitution table depending upon the key. Section 3 obtains the problem formulation and form the reverse substitution table. Design of algorithm for encryption and decryption is represented in section 4, and illustration of cipher is in section 5. The paper is observed by a conclusion in section 6.

2. ANALYSIS OF PROBLEM AND DEVELOPMENT OF SUBSTITUTION TABLE

The problem of cryptography under consideration can be formally stated as follows. Giving a plain text M and a pair of keys K_0 and K being generated by K_0, obtain the cipher text C. Find the plain text M from C by using the keys K_0 and K.
The plain text M comprises characters which can be represented by ASCII codes .The set of characters and the ASCII codes are given in table1.The row numbers of the table represent left digit(s) and the column numbers indicate the right digit of ASCII VALUE .

	0	1	2	3	4	5	6	7	8	9
3				Space	!	“	#	$	%	&	‘
4	(	)	*	+	,	-	.	/	0	1
5	2	3	4	5	6	7	8	9	:	;
6	<	=	>	?	@	A	B	C	D	E
7	F	G	H	I	J	K	L	M	N	O
8	P	Q	R	S	T	U	V	W	X	Y
9	Z	[	\	]	^	-	,	a	b	c
10	d	e	f	g	h	i	J	k	l	m
11	n	o	p	q	r	s	t	u	v	w
12	x	y	z	{	|	}	~			

0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
! “ # $ % & ‘ ( ) * + , - . / 0 1 2 3 4 5 6 7 8 9 : ; < = > ?
^] \ [Z Y X W V U T S R Q P O N M L K J I H G F E D C B A @
` a b c d e f g h I j k l m n o p q r s t u v w x y z { | } ~ \n
\t

as in

Table.2 :Blocks of Characters

In the first row we have the characters whose ASCII values lie between 32 and 63. In the second row we have the characters whose ASCII values are from 64 to 95, of course written in the reverse order. Similarly the remaining characters are in the third row. In this table \n and \ t two new characters have been included which are not given in table.1.These two characters are invariably required in program files.

For developing the encryption and decryption algorithms, let us have a key K_0 given by

K_0 = 15 4 5 9 12 14 13 11 18 19 20 21 23 17 2 3
6 7 8 10 1 16 22 24 26 28 30 31 25 27 29 0

The numbers 0 to 31 present in the K_0 correspond to the block numbers of the characters shown in the table.2. Adopt the following procedure for achieving the safety of the key. Convert numbers in the key K_0 into their binary form. Each number in its binary form will contain 5 binary bits. Here, permute the bits 1 and 5, 2 and 4, 1 and 2 and 4 and 5 of each binary number. Thus we get the key in the form.

K =	29	4	12	9	5	21	13	25	18	26	6	14	30	10	16	24
	20	18	1	17	8	2	22	3	19	7	23	31	11	27	15	0

The number 15241245 concerned to the permutation process can be considered as a key, and it may be called as Swapping key. It may be noted that the swapping of the numbers in the key K_0 will result in the same numbers in a different order. This key K can be used for process of encryption.

Basing upon the key K let us form the Substitution Table for carrying out encryption. The first number in key K is 29. It refers to the block 29 of table 2. This block contains characters '=', 'B' and '}'. Assign the numbers 0, 1 and 2 for these characters .These numbers may be called as sequence numbers. The next number in the K is 4. The block concerned to number 4 contains the characters '$', '[', 'd'. The sequence numbers for these characters are 3, 4, 5. Similarly we assign the sequence numbers for all the other characters belonging to the other blocks. The sequence number of characters in individual key K referring to table 2are placed in table 3 with reference to the row number and column number of table 1. Thus we have the substitution table (table-3) containing the ASCII codes and the corresponding sequence numbers.

	0	1	2	3	4	5	6	7	8	9
0										96
1	83									
2										
3			93	54	63	69	3	12	30	75
4	60	9	39	84	6	18	33	90	42	57
5	24	72	48	15	66	78	45	21	27	87
6	51	0	36	81	82	37	1	52	88	28
7	22	46	79	67	16	49	73	25	58	43
8	91	34	19	7	85	40	10	61	76	31
9	13	4	70	64	55	94	95	56	65	71
10	5	14	32	77	62	11	41	86	8	20
11	35	92	44	59	26	74	50	17	68	80
12	47	23	29	89	53	2	38			

Table 3: Substitution Table

Here it is to be noted that the sequence numbers of all the characters lie in between 0 and 96.Thus each sequence number can be viewed as a two digit number.

3. PROBLEM FORMULATION AND FORMULATION OF REVERSE SUBSTITUTION TABLE

Consider a block of m characters of the plain text M. Let Ai, i=1 to m, be the characters in the block. Let X_{2i-1} and X_{2i} be the tenth digit and the unit digit of the position value of Ai in table 2. As the block contains m characters the number of digits are the position (tenth & unit position)values such X_1, X_2……., X_n, where n= 2m,corresponding to each character A_i, i=1 to m. Combining the X_i values, i= 1 to n , produces the summation S. i.e.

$$S = \text{“ } Xi \quad i=1 \text{ to } n \qquad (3.1)$$

In order to make the process of ciphering more complex for security point of view assume the constant,

$$\text{i.e. } C_I = \sum_{i=1}^{n} Xi - 2X_1 = \sum_{i=2}^{n} Xi - X_1 \qquad (3.3)$$

Thus in general

$$Ci = S - 2Xi \quad \text{..... } i=1 \text{ to } n \qquad (3.4)$$

Hence it is obvious that, each Xi lies between 0 and 9. It is readily notice that the least value of C_i is -9 and the highest value of C_i is (n-1).In a similar manner, from the equation (4),we find that each C1 is in between -9 and 9(n-1).

Now consider the generated key K, comprising n numbers $k_1, k_2 \ldots . k_n$ .Adding these numbers with $C_1, C_2 \ldots \ldots C_n$ respectively, we get $d_i = C_i + K_i$, i=1,2,…n. Convert the d_i into their binary form, and each binary string corresponding to d_i is cipher text C of the plaintext M.

The process of decryption which is being adopted by the receiver can be described as follows. By considering the binary strings of specified length in the cipher text, receiver gets back di subtracting K_i from d_i, produces C_i On solving the system of simultaneous equations.

$$S - 2X_i = C_i, \text{ i=1 to n} \qquad (3.5)$$

We find

Thus obtain the sequence number i.e.(position value of ASCII characters.Hence it needs to have the reverse substitution table (Table-4) which consist of ASCII codes corresponding to the sequence number. The 1st position number represents the row number and the 2nd position number represents the column number of the substitution Table-4and so on. Intersection of both row and column number exhibits the ASCII values of each

	0	1	2	3	4	5	6	7	8	9
0	61	66	125	36	91	100	44	83	108	41
1	86	105	37	90	101	53	74	117	45	82
2	109	57	70	121	50	77	114	58	69	122
3	38	89	102	46	81	110	62	65	126	42
4	85	106	48	79	112	56	71	120	52	75
5	116	60	67	124	33	94	97	49	78	113
6	40	87	104	34	93	98	54	73	118	35
7	92	99	51	76	115	39	88	103	55	72
8	119	63	64	10	43	84	107	59	68	123
9	47	80	111	32	95	96	9			

Table 4: Reverse substitution Table

For example:
Consider a plaintext block **"binary",** where block size m=6
b i n a r y (m=6)
98 105 110 97 114 121 (ASCII value from table 1)
65 11 35 56 26 23 (Position value of each character in substitution table 3(
ASCII value of b is 98 now intersection point of 9th row and 8th column of table 3 is the position value of character b is 65))

Since, the block contain m=6, characters , the corresponding digits are (n=2m=12), X_1=6, X_2=5, X_3=1, X_4=1, X_5=3, X_6=5, X_7=5, X_8=6, X_9=2, X_{10}=6, X_{11}=2, X_{12}=3.

Then $$S = \sum_{i=1}^{12} Xi = 45,$$

Hence based on equation C_i=S-2X_i, C_1=S-2X_1=45-2*6=33, C_2=35, C_3=43, C_4=43, C_5=39, C_6=35, C_7=35, C_8=33, C_9=41, C_{10}=33, C_{11}=41 and C_{12}=39
Now select same number of keys such as K_1, K_2…., K_{12}.
Let us consider K after swapping =29 4 12 9 5 21 13 25 18 26 6 14

Now calculate $d_i = C_i + K_i$ such as
d_1=33+29=62, d_2=39, d_3=55, d_4=52, d_5=44, d_6=56, d_7=48, d_8=55, d_9=59, d_{10}=59, d_{11}=47 and d_{12}=53

The evaluated d_i is converted into binary bits which is again added with a parity bit as sentinel . Consequently binary bit and parity bit is sent to receiver.

The receiver convert the binary numbers d_i, i=1 to 12 , into their corresponding decimal numbers , after ignoring the parity bit.
Hence based on equation $C_i = d_i - K_i$., $C_1 = d_1 - K_1$=62-29=33, C_2=35, C_3=43, C_4=43, C_5=39, C_6=35, C_7=35, C_8=33, C_9=41, C_{10}=33, C_{11}=41, C_{12}=39
Then calculate the X_i by using the equation

$$X_i = (1/2)[[1/(n-2)](\sum_{i=1}^{n} C_i) - C_i], \quad i=1 \text{ to } 12$$

Hence m=6, $X_{i=}(1/2)[[1/(12-2)](450) - C_i]$, i=1 to 12 , X_1=1/2(45-33)=6, X_2=5, X_3=1, X_4=1, X_5=3, X_6=5, X_7=5, X_8=6, X_9=2, X_{10}=6, X_{11}=2, X_{12}=3
Now grouping the two digits into one to form a number from left to right manner, so , the result is 65 11 35 56 26 23.
Then by using the reverse substitution table 4 the corresponding ASCII values are 98 105 110 97 114 and 121
Now the corresponding ASCII characters are **"binary"** , this is the plain text(PT) .

4. Design Of The Algorithm

In what follows, we design the algorithms for encryption and decryption.

$$X_i = (1/2)\left[1/(n-2)\left(\sum_{i=1}^{n} C_i\right) - C_i\right], \quad i=1 \text{ to } n \qquad (3.6)$$

Algorithm For Encryption

{
1. Take the key K_0;
2. Permute the key K_0 by using the swapping key S , Then we get K;
3. Construct the substitution table basing upon K;
4. while not end of file do
{
5. Read m characters A_i ,i=1 to m,from the input file;
6. Obtain the sequence numbers N_i, i=1 to m , corresponding to the ASCII codes of the charcters, from the Substitution Table;
// Find x_i , i=1 to n , n=2m
7. for i=1 to n do
{
$X_{2i-1} = N_i / 10$; $X_{2i} = N_i \bmod 10$;
}
// Compute S
8. S=0;
for i=1 to n do
S=S+ xi ;
//Compute C_i

9. for i=1 to n do
$C_i = S - 2X_i$;
10. for i=1 to n read K_i ;
11. for i=1 to n do
$d_i = C_i + K_i$;
12. Convert d_i into their corresponding binary form and add the parity bit;
13. Write the binary strings in the output file;
}
}

Algorithm For Decryption

{
1. Permue the key K_0 by using the swapping key S , Let the permuted key be K ;
2. Construct the reverse substitution table basing upon K;
3. while not end of cipher text do
{

4. Read the binary numbers d_i, i=1 to n ;
5. Convert the binary numbers d_i, i=1 to 12 , into their corresponding decimal numbers , after ignoring the parity bit;
6. for i = 1 to n read K_i;
7. for i = 1 to n $C_i = d_i - K_i$;
8. for i = 1 to n do

$$X_i = (1/2)[1/n - 2(\sum_{i=1}^{n} C_i) - C_i];$$

9. for i = 1 to m do
$N_i = 10X_{2i-1} + X_{2i}$;
10. Obtain the ASCII codes corresponding to the sequence numbers N_i, i=1 to m from the reverse substation table;
11. Write the charcters A_i, i=1 to m , in the output file;
}
}

5 Illustration of the cipher

Take a text file as input. Use the Encryption and Decryption algorithms on the same text file. Now, we have to observe what will be the corresponding output or cipher text.

Let , the key K_0 = 15 4 5 9 12 14 13 11 18 19 20 21 23 17 2 3
6 7 8 10 1 16 22 24 26 28 30 31 25 27 29 0

Then, the swapping key K will be
K = 29 4 12 9 5 21 13 25 18 26 6 14 30 10 16 24
20 18 1 17 8 2 22 3 19 7 23 31 11 27 15 0

Input Plain-Text

The concept of information will be taken to be an understood quantity. To introduce cryptography, an understanding of issues related to information security in general is necessary. Information security manifests itself in many ways according to the situation and requirement. Over the centuries, an elaborate set of protocols and mechanisms has been created to deal with information security issues when the information is conveyed by physical documents.

The corresponding Cipher text using the algorithm is obtained as:

CRYPTANALYSIS

In this thesis, we have introduced the keys K_0, K and swapping key(*s*) have been introduced. Some of these can be kept safely with the receiver and some can be transmitted to him in a secret manner. It is seen that substitution table and the reverse substitution table both depend upon K which is being obtained from K_0 and *S*. Thus supplying K_0 and S by different mechanisms or at different instances, in parts , would ensure the security of the algorithm quite significantly.

.

Let us focus our attention specifically on a block of plain text and the corresponding ciphertext. From the lengths of the blocks of the plain text and the cipher text, we can readily calculate the number of binary bits reprenting each $d_i(=C_i + k_i)$ and the the values of each d_i.

Let us consider the instance when the length 0f plain text block is 6. In this case we obtain the values of d_i, i=1 to 12. Then the values of C_i, i= 1 to 12, can be calculated only when the numbers k_i, i=1 to 12 are known.

As it has been pointed out in section 3, when n=6 the least value of C_i is -9 and greatest value of C_i is 99. In order to see that no d_i requires more than 7 binary bits for its representation, for brevity of the ciphertext, we must have the values of d_i, in the range 0 to 127. To this end, we are to select the values of k_i such that they lie between 9 and 28. Thus each k_i can be chosen in 20 ways. As each k_i can be selected in 20 ways , the size of the space of key k is 20^{12} .

Hence even after attacking with all possible choices of k_i , it may not be possible to determine x_i. Uniquely. This may happen on account of the fact that we may get one set of integral values of X_i for one set of values of C_i, and another set of integral values of x_i for some other set of values of C_i.

Fortunately if we are able to obtain the values of x_i uniquely by considering all the cases in an exhaustive manner we can readily find the sequence numbers corresponding to the characters in the block. By considering some more blocks in a similar manner it will be possible to find the substitution table and reverse substitution table which will enable us to break the cipher. However let us now estimate the time required for obtaining x_i in 20^{12} cases in the case of a single block of plain text.

Let us suppose that we can determine x_i corresponding to one set of values of k_i in 10^{-6} sec. Then in the worst case obtaining x_i in the case of one block, we require $20^{12} \text{ X } 10^{-6}$ sec =133 years. As this process is to be repwated for several blocks, say b blocks, the time required for the computation of x_i in the case of all the blocks is 133 b years.

In order to increases the strength of algorithm we can select k_i from the range 9 to 156 instead of 9 to 28. Then the values of d_i lie in the range 0 to 255. Thus, we require 8 bits for the representation of d_i. In this case the size of the key space of k is $(148)^{12}$. Then the time required for finding x_i in this case is $= (148)^{12} \text{ X } 10^{-6} = 11 \text{ X } 10^{19}$ years. This shows that breaking the algorithm by the known plaintext attack is ruled out.

Letus now consider the second case. In this , as we know only cipher text, we do not have any other option except to attack the cipher by brute-force approach. In the key K we have the numbers 0 to 31. As there is

no repetition of the numbers in the key, the size of the key space is $_{-\%32}$. Considering each key we have to adopt the following procedure to determine whether the key under consideration is the correct one or not.

We form substitution table by using the key.For each possible block of 6 characters, we make use of the sequence numbers and obtain C_i. Then , assuming all possible values of k_i we have to check whether $C_i + k_i$ matches with d_i which is known to us from the cipher text. This process consumes a very long time. If we assume that the process takes 1 sec (which is impossible) the time required to carry out the brute-force attack with all the possible keys is $_{-\%32}$ sec $= 7616 \text{ X } 10^{32}$ centuries.

In order to increase the strength of the algorithms enormously we change the value of the key k from block to block i.e, we use one set of values for k_i, i=1 to n , with the first block, another set of values with the second block and some other set of values with the third block. Thus we restrict ourselves only to three sets of values of k_i and repeat the usage of three keys with all other blocks cyclically.

6. FUTURE WORK

Our experimental result shows the encryption and decryption of text file using linear algebric equation. In future, we will make a comparision with other Symmetric Cipher Algorithm and our aim is to make it as the best algorithms among others. Again we also prove its correctness taking a large amount of data.

7. CONCLUSION

In this paper we have developed a pair of novel cryptographic algorithms by using multiple keys. Both the algorithms depend upon the computation of simple algebraic equations. The algorithms mainly depend upon two keys , namely K_0 and K. From the result analysis we conclude that the algorithms are highly potential in all respects.

REFERENCES

[1] V. U. K. Sastry, D. S. R. Murthy, S. Durga Bhavani, "*A Modified Feistel Cipher involving Modular Arithmetic and a Key on both the sides of a Plain Text Matrix*", International Journal of Computational Intelligence and Information Security, Vol. 1, No. 4, Jun. 2010

[2] V. U. K. Sastry, D. S. R. Murthy, S. Durga Bhavani, "A Novel Block Cipher involving Feistel structure and Modular Arithmatic" International Journal of Computational Intelligence and Information Security, Vol. 1, No. 4, page 48-54Jun. 2010

[3] Bruce Schneier, "Applied Cryptography ", John Wiley 1996.

[4] AD.E.Denning " Cryptography and Data Security ", Addision Wesley 1982.

[5] William Stallings " Cryptography and Network Security " Pearson Education,2002

[6] W. Alexi, B. Chor, O. Goldreich, and C.P. Schnorr, RSA and Rabin functions: Certain parts are as hard as the whole, *SIAM Journal of Computing* (2) 17 (1988),

[7] M. Blum and S. Goldwasser, An efficient probabilistic public-key encryption scheme which hides all partial information, *Advances in Cryptology — Crypto '84*, Springer-Verlag (1985).

[8] American National Standards Institute, *American National Standard X3.106-1983 (R1996): Data Encryption Algorithm, Modes of Operations for the*, 1983.