A Block Cipher Containing an Attribute involved Key based Permutation and Substitution

G. Sumalatha[1], D.S.R. Murthy[2]
[1]SreeNidhi Institute of Science and Technology
[2]Geethanjali College of Engineering and Technology
(E-mail: sumalathagunnala23@gmail.com)

***Abstract*—** In this analysis we have developed a block cipher, by introducing a pair of functions, namely (1) Permute(), and (2) Substitute (). The function Permute () depends upon the number in the serial order of the elements in the key , and the number corresponding to the ascending order of the numbers in the key. The function Substitute() is based upon the Matrix, containing the Key at the beginning and the rest of the numbers in subsequent positions in a serial order, and a set of rules which are applicable for replacing a pair of numbers in the plaintext. In the proposed scheme, the key is computed from the credentials of the user such as email or social security number. The iteration process involved in the analysis and the functions Permute() and Substitute() strengthen the cipher significantly.

***Keywords*—** *Attributes, Cipher, Information security, Key, Permute, Substitute.*

I. INTRODUCTION

Several years back, Charles Wheatstone[8] developed a multiple letter encryption cipher, called Playfair cipher. This cipher depends upon a 5X5 matrix of letters, consisting of the letters of the keyword at the beginning and the rest of the letters, in a sequential manner, at the subsequent positions of the matrix. The matrix is obtained in the following form.

M	O	N	A	R
C	H	Y	B	D
E	F	G	I /J	K
L	P	Q	S	T
U	V	W	X	Z

Here MONARCHY is the keyword.

The set of rules governing the encryption of pairs of letters is as follows.

1. Repeating plaintext letters that are in the same pair are separated with a filler letter, such as x. For example balloon would be treated as balxloxon.
2. Two plaintext letters that fall in the same row of the matrix, each replaced by the successive letters to the right , circularly following the last if needed. For example AR is encrypted as RM.
3. Two plaintext letters that fall in the same column of the matrix, are replaced by the successive letters in the downward direction of the column, circularly following the column if needed. For example MU is encrypted as CM.
4. Each plaintext letter in a pair is replaced by the letter that lies in its own row and the column occupied by the other plaintext letter. For example HS is encrypted as BP and EA encrypted as IM (or JM, depending upon the wish of the encipher).

For quite a long time this cipher, called Playfair cipher, was found to be very strong as there were 26x26=676 digrams involved in the process. However, subsequently it could be broken by using the frequency distribution of letters.

In recent investigations [1, 6, 7], the Playfair cipher is modified to some extent by considering EBCDIC code instead of alphabet in the development of the matrix. In [3- 5], the block ciphers are developed by using the permutation process basing upon the key. The ciphers developed in [1, 3-7], uses the key contains the random values. Recently, Sumalatha Gunnala et al. [2] introduced the attribute involved keys in encryption process. Here the encryption process includes additional key element derived from the unique identity of the user such as email, social security number or Aadhaar etc. In this present analysis our objective is to study a modified Playfair cipher by using key involved permutation process. And the key is computed by using the attribute values of the user instead of random numbers. The attributes included as email or social security number etc. Thus this feature provides the authenticity of the sender.

The plan of the paper mentioned as follows. The Section 2 deals with the formulation of the problem, with the algorithms. The illustration of the problem is presented in section 3.The cryptanalysis is discussed in section 4. Finally the results and conclusions drawn in section 5.

II. FORMULATION OF THE PROBLEM

Corresponding to the EBCDIC code we have 256 numbers which can be written in the form of a square matrix of size 16.

Let us consider a key K containing 16 numbers. Let the key be given by

K= [98 209 49 4 161 128 154 252 70 117 89 36 22 153 182 197] (1)

On placing the key at the beginning of the matrix, and the remaining numbers of the EBCDIC code (0 – 255) , one after another in a sequential manner, in the subsequent positions , we get a matrix M, having the following form.

TABLE 1. Substitution Table

	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**
1	98	209	49	4	161	128	154	252	70	117	89	36	22	153	182	197
2	0	1	2	3	5	6	7	8	9	10	11	12	13	14	15	16
3	17	18	19	20	21	23	24	25	26	27	28	29	30	31	32	33
4	34	35	37	38	39	40	41	42	43	44	45	46	47	48	50	51
5	52	53	54	55	56	57	58	59	60	61	62	63	64	65	66	67
6	68	69	71	72	73	74	75	76	77	78	79	80	81	82	83	84
7	85	86	87	88	90	91	92	93	94	95	96	97	99	100	101	102
8	103	104	105	106	107	108	109	110	111	112	113	114	115	116	118	119
9	120	121	122	123	124	125	126	127	129	130	131	132	133	134	135	136
10	137	138	139	140	141	142	143	144	145	146	147	148	149	150	151	152
11	155	156	157	158	159	160	162	163	164	165	166	167	168	169	170	171
12	172	173	174	175	176	177	178	179	180	181	183	184	185	186	187	188
13	189	190	191	192	193	194	195	196	198	199	200	201	202	203	204	205
14	206	207	208	210	211	212	213	214	215	216	217	218	219	220	221	222
15	223	224	225	226	227	228	229	230	231	232	233	234	235	236	237	238
16	239	240	241	242	243	244	245	246	247	248	249	250	251	253	254	255

In the process of encryption, the set of rules used for substitution of pairs of numbers are as follows.

1. If both the numbers in a pair of numbers are the same, both are replaced by the adjacent number either following the row or column in the matrix.
2. If two numbers are distinct and fall in the same row of the matrix, then each one is replaced by the number to its right, with the first element of the row circularly following the last, if required.
3. If two numbers are distinct and fall in the same column of the matrix, then each one is replaced by the successive numbers in the downward direction of the column, circularly following the column, if needed.
4. Otherwise, each number in a pair is replaced by the number that lies in its own row and the column occupied by the other number. That is, if we have the first number in a pair is ith row jth column element, and the second number is r^{th} row sth column element, then the first number will be substituted by the ith row sth column element, and the second number will be substituted by r^{th} row j^{th} column element.

The basic steps involved in the process of the encryption are

P = Permute(P , K),

P= Substitute(P , M),

C=P.

The corresponding decryption process is given by

C= ISubstitute(C, M),

C=IPermute(C,K),

P=C.

Here P denotes the plaintext, and C denotes the ciphertext. The function Permute() represents a process of interchange of the numbers corresponding to the characters of the plaintext. This interchange depends upon the key K. The function Substitute() depends upon the matrix M, and the numbers corresponding to the characters in the plaintext.

IPermute ( ) and ISubstitute ( ) denote the reverse processes of Permute() and Substitute() respectively.

Now let us have a clear insight into the process of the function Permute().

We consider a plaintext P given by

P = Dear Sir! Many. (2)

On writing this in terms of the EBCDIC code, we have

P= 64 196 133 129 153 64 226 137 153 79 64 212 129 149 168 64. (3)

By introducing a serial number (SN), and a number (NA), corresponding to the ascending order of the numbers in the key, K can be written as shown in the following Table.

TABLE 2. Permutation Table

SN	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Key	98	209	49	4	161	128	154	252	70	117	89	36	22	153	182	197
NA	7	15	4	1	12	9	11	16	5	8	6	3	2	10	13	14

This Table suggests that we can permute 1st number with the 7th number, 2nd with the 15th , 3rd with 4th , 5th with 12th , 6th with 9th , 8th with 16th , and 14th with 10th . Further, we notice that the numbers in the 11th and 13th positions will not undergo any change . Here it is to be noted that a number once interchanged will not undergo any change further. In the light of this, the plaintext P, given by (3) ,assumes the form, P = 226 168 129 133 212 153 64 64 64 149 64 153 129 79 196 137. (4)

It is worth noticing that the function Permute( ) and IPermute( ) will lead to the interchange of the same numbers, and hence they can be taken as the same.

Now let us consider the process of substitution ():

In the couple of numbers (226 , 168) , 226 is the element of 15th row 4th column of the Matrix M, and 168 is the element of 11th row 13th column. Thus according to the rule (4), 226 will be replaced by the element of 15th row 13th column of the Matrix, i.e. by 235,and 168 will be replaced by the element of 11th row 4th column of the Matrix, i.e by 158.Similarly the pairs (212,153), (64,153) (129 ,79) ,(196 ,137) will be replaced by the corresponding pairs. In accordance with the rule (1), the pair (64,64) will be replaced by the pair (65,65). The numbers in the pair (129, 133) are in the same row. Hence according to rule (2), they will be replaced by the corresponding adjacent numbers 130 and 134 respectively. The numbers 64 and 149 are in the same column. Hence according to rule (3), they will be replaced by 81 and 168 respectively. Hence after substitution, we obtain the plaintext in the form

P = 235 158 130 134 220 128 65 65 81 168 65 22 131 77 189 144 (5)

This process is repeated r number of times, where r is taken as 16, in the present analysis. On performing decryption we get back the plaintext P, if it is not interrupted in between.

The algorithms of Encryption and Decryption are given below.

Algorithm for Encryption:

1. Read P, K,M, r
2. for i= 1 to r do
   {
3. P=Permute(P,K)
   P =Substitute(P,M)
   }
4. C=P
5. Write(C)

Algorithm for Decryption:

1. Read C, E, M, r
2. for i = 1 to r
   {
3. C =ISubstitute(C,M)
   C= IPermute(C,K)
   }
4. P=C

III. ILLUSTRATION OF THE PROBLEM

Consider the plaintext given below.

Dear Sir! Many changes are coming in Kashmir. Several Hindus are migrating to other parts of the India, so that they and their families can comfortably reside along with all the other Hindus. This sort of migration is a matter of encouragement for all Muslims. We can send some of our Pakistanis into Kashmir by offering them some encouragement whole heartedly. We can request some of our Muslim friends, staying in India, to come to Kashmir by providing them some facilities for their stay and business. This process will definitely help us in occupying Kashmir. All the while struggling with weapons is not the appropriate solution. Please take necessary decision in respect of this issue. Yours sincerely, XXX. (6)

On focusing our attention on the first 16 characters, we have a block of plaintext given by

P= Dear Sir! Many . (7)

After completing the first round of the iteration process, the plaintext assumes the form,

P = 235 158 130 134 220 128 65 65 81 168 65 22 131 77 189 144 (8)

Following the same procedure, on performing the sixteenth round of the iteration, i.e. at the end of the encryption, we obtain

C= 129 , 224 , 133 , 129 , 31 , 133 , 48 , 203 , 65 , 113 , 99 , 6 , 164 , 219 , 193 , 100 (9)

On performing decryption of the ciphertext given in (9), we get the corresponding plaintext P.

IV. CRYPTANALYSIS

The validity of a cipher can be determined by examining cryptanalysis. The various types of approaches in the cryptanalysis are

a) Ciphertext only attack (brute force attack),
b) Known plaintext attack,
c) Chosen plaintext attack,
d) Chosen ciphertext attack.

In the development of every cipher, one has to take care of that it sustains at least the brute force attack, and the known plaintext attack [7].

The key is containing 16 decimal numbers. Thus the size of the key space is 2^{128}.

Let us assume that the time required for the computation of the cipher with one value of the key is 10^{-7} seconds. Then the time required for the computation with all the possible values of the key in the key space is

$$\frac{2^{128} \times 10^{-7}}{365 \times 24 \times 60 \times 60} = \frac{10^{38.4}}{365 \times 24 \times 60 \times 60} = 3.12 \times 10^{23.4} \text{ years} \qquad (10)$$

As this number is enormously large, it is not possible to break the cipher by the brute force attack.

Let us now examine the known plaintext attack.

If we confine our attention to only one round of the iteration process (i.e when r=1), we have the equations describing the cipher in the form .

$$P = \text{Permute}(P, K) \qquad (11)$$
$$P = \text{Substitute}(P, M) \qquad (12)$$
$$C = P \qquad (13)$$

In the known plaintext attack, the pair of the ciphertext and the plaintext are known to us. Even then we cannot determine the key K by any means. Thus this cipher cannot be broken by the known plaintext attack.

Here it is not possible to choose a plaintext and/or ciphertext to break the cipher. From the above analysis we conclude that the cipher is unbreakable.

V. RESULTS AND CONCLUSIONS

In this investigation we have developed a block cipher, cipher, by using the functions Permute( ) and Substitute( ). Due to the function Permute ( ), the numbers in the plaintext undergo several interchanges and this process is developed based on the key. Here the key is calculated from the credentials, called attributes of the user such as email or social security number. With this feature the sender's authenticity is provided at receiver side. On account of Substitute ( ), the adjacent numbers change in an appropriate manner. In this scheme there are 256 numbers, thus 256 X 256 (i.e. 2^{16}) pairs of numbers are replaced appropriately. As there are 16 rounds in the development the procedure for the encryption, the strength of the cipher is expected to be commendable.

The plaintext given (6) is divided into 45 blocks, wherein each block is of size 16 characters. As the last block is having 3 characters, we have appended 13 characters, of our choice, so that it becomes a complete block. Here we have appended the string sumalathasuma. The ciphertext of each block , presented in(14).

Here it is to be noted that the strength of the cipher enhances due to the functions Permute( ) and Substitute( ), and the number of rounds in the iteration process.

REFERENCES

[1] P. Murali, and G. Senthilkumar, Modified version of playfair cipher using linear feedback shift register, International Journal of Computer Science and Network Security, vol. 8, no.12, pp. 26-29, 2008.

[2] Sumalatha Gunnala, Shirisha Kakarla and Sreerama Chandra Murthy Dasika , "An Attribute Involved Public Key Cryptosystem Based on p-Sylow Subgroups and Randomization" , Journal of Applied Computer Science & Mathematics , vol. 12, Issue 1/2018, pp 34-38, 2018.

[3] V.U.K. Sastry, K.Shirisha, "A Novel Block Cipher Involving a Key bunch Matrix and a Key-based Permutation and Substitution", International Journal of Advanced Computer Science and Applications (IJACSA), Vol. 3, No. 12, pp. 116-122, 2012.

[4] V.U.K. Sastry, K.Shirisha, "A Block Cipher Involving a Key Bunch Matrix and an Additional Key Matrix, Supplemented with XOR Operation and Supported by Key-Based Permutation and Substitution", International Journal of Advanced Computer Science and Applications (IJACSA), Vol. 4, No. 1, pp. 187-194 , 2013.

[5] V.U.K. Sastry, K.Shirisha, "A Block Cipher Involving a Key Bunch Matrix and an Additional Key Matrix, Supplemented with Modular Arithmetic Addition and supported by Key-based Substitution", International Journal of Advanced Computer Science and Applications (IJACSA), Vol. 3, No. 12, pp. 110-115, 2012,

[6] V. U. K. Sastry, N. R. Shankar, and S. D. Bhavani, A modified playfair cipher for a large block of plaintext, International Journal of Computer Theory and Engineering, vol. 1, no. 5, pp. 592-596, 2009.

[7] V. U. K. Sastry, N. R. Shankar, and S. D. Bhavani, A modified playfair cipher involving interweaving and iteration, International Journal of Computer Theory and Engineering, vol. 1, no. 5, pp. 597-601, 2009.

[8] William Stallings, "Cryptography and Network Security", Fourth Edition , Pearson ,2007.

G. Sumalatha is currently working as Associate Professor in the Department of Information Technology, SreeNidhi Institute of Science and Technology (SNIST), Hyderabad, India. She is pursuing PhD in JNTUH. Her research interests include Information security, cryptography, data analytics and compilers. She published thirteen research papers in reputed International Journals.

Dr. D.S.R. Murthy is presently working as Professor in the Department of Computer Science and Engineering (CSE), Geethanjali College of Engineering and Technology, Hyderabad, India. He published a text book on **C and Data structures.** He also published number of research papers in various international journals.

129	224	133	129	31	133	48	203	65	113	99	6	164	219	193	100
122	123	129	149	143	135	166	52	151	46	166	100	172	151	152	145
143	125	64	137	163	86	222	135	205	151	174	189	15	111	53	234
129	202	133	153	130	152	65	235	138	149	134	160	171	65	183	44
169	94	148	137	155	21	203	237	158	139	169	86	156	158	95	186
163	129	133	153	102	155	136	252	171	198	84	137	189	96	169	136
185	133	201	149	131	152	137	137	56	170	151	53	171	123	131	165
100	222	136	133	180	106	206	217	203	135	173	188	157	188	102	136
125	133	148	137	149	139	120	166	118	185	131	170	83	133	138	140
238	169	153	163	129	130	237	221	66	197	122	171	137	129	169	138
131	149	150	149	120	64	171	147	165	136	87	166	137	149	65	158
136	130	64	150	155	164	137	1	99	200	137	185	134	198	181	101
114	236	136	137	182	134	189	179	118	10	204	15	230	134	150	193
180	22	129	163	188	151	179	101	158	175	130	166	55	152	133	220
222	172	153	64	221	187	86	167	167	172	165	168	31	136	155	155
156	171	149	163	100	165	187	0	116	187	201	201	151	25	205	164
149	141	148	162	111	118	8	155	132	186	144	186	82	199	159	157
169	101	162	150	137	141	99	146	152	66	171	200	32	118	253	130
140	143	162	163	166	192	146	167	69	188	183	188	204	135	218	122
202	150	148	137	66	135	151	174	101	186	187	169	187	67	139	171
131	64	163	136	174	155	65	170	210	172	17	239	177	173	126	149
153	65	129	135	135	149	235	198	171	53	165	135	152	147	187	100
159	159	129	153	230	202	172	189	235	143	133	25	202	133	169	160
222	146	153	133	152	164	205	221	163	64	162	150	148	133	171	222
134	57	150	164	13	60	206	169	170	171	170	148	83	121	70	149
184	192	132	162	108	61	221	188	136	156	139	137	136	63	199	171
101	197	149	132	167	151	151	110	172	149	61	150	150	143	170	84
155	138	64	210	145	186	121	146	137	153	115	181	185	76	137	182
190	210	137	132	152	151	137	99	165	136	157	174	83	180	152	156
222	151	134	129	122	141	173	238	201	188	120	158	72	147	187	84
56	171	136	133	166	12	52	166	158	148	205	102	171	157	136	52
130	171	162	137	219	168	168	162	116	127	5	152	196	173	53	149
51	170	131	133	166	170	122	205	141	139	151	52	123	124	170	184

149	139	163	133	155	164	56	125	173	151	187	121	155	162	56	145
169	103	150	131	126	205	173	204	141	151	121	57	250	201	237	163
148	137	153	75	99	21	143	147	168	196	171	235	99	89	136	141
139	124	64	162	165	197	155	126	120	149	139	151	120	66	157	145
224	140	64	166	167	169	151	151	152	176	81	137	191	102	148	190
167	52	163	136	139	102	133	139	157	13	143	138	51	206	120	171
171	140	162	150	149	166	238	233	152	151	77	66	217	149	222	188
188	184	64	163	135	152	171	145	254	171	152	217	170	170	137	32
253	92	132	133	176	221	22	202	150	149	106	187	139	102	34	185
195	168	133	131	157	66	174	168	55	165	131	152	170	56	158	190
170	164	133	75	67	234	152	157	16	164	102	215	139	151	135	124
197	132	147	168	132	62	52	238	223	223	127	85	56	64	64	52
97	145	64	162	168	152	184	202	120	171	123	129	162	168	232	168

(14)