International Journal of Mathematical Archive-2(10), 2011, Page: 2084-2089
Available online through www.ijma.info ISSN 2229 – 5046

A SURVEY ON RECENTLY MODERNIZED CRYPTOGRAPHIC ALGORITHMS AND ANALYSIS ON THE BLOCK CIPHER GENERATION USING PLAY COLOR CIPHER ALGORITHM

***Kallam Ravindra Babu[1], Dr .S. Udaya Kumar[2], Dr. A. Vinaya Babu[3]**

[1]Research Scholar (JNTUH),HOD CSE&IT, AZCET, Mancherail, A.P, India
[2]Principal, M. V. S. R. Engineering College, Hyderabad, Andhra Pradesh, India
[3]Director, Admissions, JNTUH, Hyderabad, A.P, India

rbkallam2510@gmail.com, uksusarla@rediffmail.com, avb1222@gmail.com
(Received on: 14-10-11; Accepted on: 03-11-11)

ABSTRACT

I*n this paper we have presented the review on recently updated Playfair, Poly Alphabetic and RSA Cryptographic algorithms. We have also analyzed the block cipher generation using play color cipher algorithm along with its six variants.*

Keywords: *Cipher, Steganography, Cryptography, Substitution, Transposition, Poly Alphabetic, Play fair, PCC.*

1. INTRODUCTION:

The extremely prevailing and universal approach to defense the threats to information security is encryption [1]. The process of converting plaintext into cipher text (encryption) and cipher text to plain text (decryption) is called Cryptography. Yet it is very authoritative, the cryptanalysts are very sharp and were functioning seriously to break the ciphers. To face the cryptanalyst in the battle of network and information security, it is obligatory to modernize the existing algorithms or invent new algorithms. In the recent past Udaya et al, have updated few algorithms [4] and invented a new cryptographic algorithm by name it is "Play Color Cipher" [10].

In the upcoming section we are going to present the recent updates of Playfair, Poly alphabetic, RSA algorithms and the survey on play color cipher and its six versions.

2. PLAYFAIR CIPHER ALGORITHM:

It is preeminent multiple-letter cryptographic algorithm, based on the use of a 5X5 matrix (Figur-1) of letters build using keyword. In this case, the keyword is MONARCHY. The matrix is built by inserting letters of the keyword from left to right and from top to bottom, and then filling in the rest of the matrix with the left over letters in alphabetic order[2][3].

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

Figure: 1 A 5X5 Matrix for Play Fair Cipher

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

Figure: 2 A 5X5 Matrix for Play Fair Cipher

The letters I / J considered as one letter. Plaintext is encrypted two letters at a time according to the policy:

- Repeating plaintext letters that would fall in the same pair are separated with a filler letter, such as x, so that balloon would be enciphered as ba lx lo on.

***Corresponding author:** *Kallam Ravindra Babu[1], *E-mail: rb_kallam@yahoo.com*

- Plaintext letters that fall in the same row of the matrix are each replaced by the letter to the right, with the first element of the row circularity following the last. For example, ar is encrypted as RM
- Plain text letters that fall in the same column are each replaced by the letter beneath, with the top element of the row circularly following in the last .for example, mu is encrypted as CM.
- Otherwise, each plaintext letter is replaced by the letter that lies in its own row and the column occupied by the other plaintext letter. thus, hs becomes BP, and ea becomes IM (or JM, as the enciphered wishes).

If the plain text is "ba lx lo on", its corresponding cipher text will be "IBSUPMNA" or "JBSUPMNA".

In the above algorithm Udaya et al, have noticed few drawbacks and shown way out for the same in their papers [4]. The problems they have noticed and the solutions are:

Case-1: The plain text preferred for renovation should have even number of characters otherwise, we can not divide the given text into the pairs of characters.

Example: if the plain text is" meaning" it will be divided as "me an in g", because it is having " 7 " characters the last character 'g' is single character and the discoverer of this algorithm have not measured this dilemma.

The simple solution shown by Dr. Udaya et al, for the case 1 is, append a letter 'X' right to the last letter in the text, so that the number of characters in the text will become even and can be encrypted[5].

Case 2: In the 5X5 matrix, since we have only 25 entries, the letters I / J counted as one letter. If we encrypt the plain text which is having the letter I / J and when we decrypt the cipher text at the receiving end, the receiver will be under uncertainty whether to consider I or J in his text, because the significance can be tainted with the change of the letter.

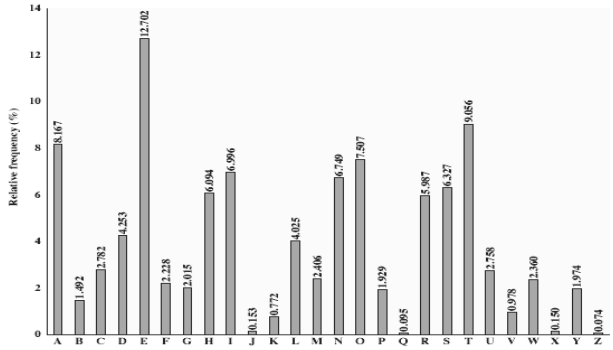

Figure: 3 Relative frequencies of letters in English text

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	0	1	2	3
4	5	6	7	8	9

Figure: 4 A 6X6 Matrix for Play Fair Cipher

We can observe that, the relative frequency of letters can be determined and compared to a standard frequency distribution for English, as shown in the figure-3 (based on [LEWA00]). From the figure 3 it is noticed that, the frequency of the letter I is 6.996 and J is 0.153. These are widely used letters in normal text [3] and considered as a single letter in the Playfair Figure-1. It may leads to the confusion at the receiving end.

Example: If the plain text is "Jam", after encryption when it is decrypted it can be "I am" instead of *Jam*. It is observed that the meaning of the word will be changing after decryption, because of the vagueness of I/J letters and also because of the space character.

In Defense services, each message is very critical and have a lot of risk involves, in such a case the receiver should not have a choice to select a letter in the text, they should obey their superior order, otherwise that may leads to lot of problems.

To reduce the ambiguity at the receiving end; it is better to combine the lees frequency letters as a one letter in the Figure 1 rather then using I/J as single letter. So, that the less frequency letters appears very rare in the text and hence we can reduce the confusion level while decrypting at the receiving end. For this Dr. Vinaya et al, recommend [4] to combine Q (0.095) and Z (0.074) as a single letter in the matrix as shown in figure 2.

Because the character Q and Z appears very rare in the plain text, the receiver faces very less confusion while decrypting. To avoid complete confusion in Case 2 and to consider alphanumeric characters in message for conversion,

in his paper Kallam et al, have suggested[5] and constructed a 6 X 6 matrix with 26 alphabets and 10 decimal numbers as shown in figure 4. With this the authors have given the solution for most of the problems encountered in Playfair cipher algorithm.

3. POLY ALPHABETIC CIPHER ALGORITHM:

Vigenere cipher is one of the renowned algorithms in poly alphabetic cipher. In this algorithm a table of alphabets can be used for both encryption and decryption, termed as Vigenere table. It consists of the alphabet written out 26 times in different rows, each alphabet shifted episodically to the left compared to the previous alphabet, corresponding to the 26 possible Caesar ciphers.

Each cipher is denoted by a key letter, which is the cipher text letter that substitutes for the plaintext letter a. Each of the 26 ciphers is laid out horizontally, with the key letter for each cipher to itself. The Vigenere table is as shown in Figure 5.

	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
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
b	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	A
c	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
d	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
e	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
f	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
g	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
h	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
i	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
j	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
k	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
l	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
m	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
n	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
o	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
p	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
r	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
s	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
t	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
u	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
v	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
w	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
x	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
z	Z	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

Figure: 5 A Vigenere table of matrix 26X26

At different points in the encryption or decryption processes, the cipher uses a different alphabet from one of the rows of the Vigenere table. The alphabet used at each point depends on a repeating keyword. For encrypting a message or plaintext the user should chose a key by satisfying the condition that the length of the key should be equal to the length of the plaintext. For a given key letter *x* and the plain text *y*, the cipher text letter is at the intersection of the row labeled *x* and the column labeled *y*; in this case the cipher text is V.

Decryption is equally simple. The key letter again identifies the row. The position of the cipher text letter in that row determines the column, and plaintext letter is at the top of the column. For example the plain text is: *"an ice image"*

The sender of the message chooses a keyword and repeats it until its length matches with the length of the plaintext, for example, the keyword *"lemon",* then the key will be: "lemonlemon"

The first letter of the plaintext is 'a', can be enciphered using the alphabet in row 'l', which is the first letter of the key chosen. The cipher letter is the intersection of the row 'l' and column 'a' of the Vigenère square, here it is 'L', and it will continue as shown below. The cipher text for the chosen plaintext will be 'LRXQRTQMUR'. For decryption select the row based on the key letter, finding the position of the cipher text letter in that row, and use the corresponding column label as the plaintext.

Plaintext:	`aniceimage`
Key:	`lemonlemon`
Cipher text:	`LRXQRTQMUR`

It is to be observed that, the existing algorithm do not consider the space in the sentence while converting. Hence the receiver will be under ambiguity where to insert the space in the available text, because there is a possibility of forming two different sentences with different meaning with the same decrypted text. It can be observed from the above example that the plain text can be any of the following: 1. a nice image 2. an ice image.

In security services, each communication is very critical and has a lot of hazard involves, in such a case the recipient should not be in vagueness. In order to conquer this difficulty, Kallam et al [6], have anticipated an enhanced poly alphabetic cipher with extended vigenere table. For this they have added a new symbol' ƹ 'into the row and column of the Vigenere Tableau, which is not in use worldwide. The new symbol can be used to represent or to locate the blank space in the plaintext. Hence the user can easily encrypt or decrypt the message or plaintext with out any ambiguity.

With this, it is mandatory for the sender to use the special invented symbol in the plaintext where ever the space is needed and then it can be encrypted as usual. The plain text in the previous example"an ice image" should be first written as "anƹiceƹimage" and can follow the same procedure as before. After decryption at the receiving end the receiver must remove the space characters in the text and hence, he will get the actual plain text.

In the recent past, Udaya et al, have found that the existing Vigenere table is not fit for the message formed with alphanumeric characters and key board symbols. In their latest investigation they have shown the solution for same[7], for this, they built a table as 68x68 matrix, in which they have considered alphabets (1 to 26), numbers (0 to 9) and all the symbols existing on the Key board (32). To realize the course of substitution we have considered the key and the plaintext as mentioned and the corresponding cipher text is shown below:

Key: t e m p e r a t u r e 1

Plain text (alphanumeric): c = 5 /9 * (f - 3 2)

Cipher text: V # $ L ~ /(Y | & 6 I

In their current investigation Ravindra et al, have even developed a new Vigenere table of 256x256 matrix [8] and named it as a comprehensive Vigenere table with 128 ASCII and 128 Extended ASCII characters. In the results they have proven that the algorithm is fit for any kind of message, key can be any combination of 256!, **brute force approach** is not possible, it is un breakable by the crypt analyst and hence the cipher is very strong.

4. RSA ALGORITHM:

RSA is the famous asymmetric cryptosystem which is based on arithmetical functions rather than on simple operations on bit patterns. It is block cipher in which plain text and the cipher text are the integers between 0 and n-1 for some n. It begins by selecting two prime numbers, p and q and calculating their product n, which is the modulus for encryption and decryption. In this each user has to generate Private/ Public key pair[2]. The weakness of this algorithm is to factorize (n) which is the product of two unequal primes (p & q).

In his research Aboud and AL-Fayoumi [9] tried analysis the algorithm reversely. Coppersmith [9] introduced a new type of attacks on RSA which capacitate a passive adversary to recover such message from the corresponding cipher text. Hastad [9] made an attack on RSA with small key. Wiener [9] proposed an attack hinges about find the *d* value directly with special case of *d*, the RSA secret exponent *d* is chosen to be small compared to the RSA modulus *N*. A well-known attack on RSA with low secret-exponent *d* was given by Wiener about 15 years ago. In the recent past Prof. Alaa invented a new method[9], and mentioned that he can break the RSA in 953 milliseconds of length 'n' with 180 digits, where n is the product of two unequal prime numbers. Many more scientists were working round the clock to break the RSA in better time.

To strengthen and to endure from the attacks, Udaya et al, have improved the existing algorithm by altering the p and q[10]. Instead of two unequal prime numbers in this they have considered p as a prime number and q as a non-negative integer. An enhanced algorithm is explained here with an example:

Considered, p=13 (prime number) and q=20 (non negative integer)

Step1: Compute n=p x q = 13 x 20 =2 60.

Step2: Compute Ø (n) = (p-1) x (q-1) = 12 x 19 = 288.

Step3: Compute *e* such that *gcd (e, Ø (n)) = 1*.

gcd (5, 528) = 1, hence e=5;

Step4: Compute d such that *de = 1mod Ø (n),* using the Extended Euclidean algorithm the generated value of d is 137. With this the Public Key (KU) = {e, n} = {5, 260} and the Private Key (KR) = {d, n} = {137, 260}

It is noticed that the algorithm is working properly with out any burden on the existing system. It is confirmed that, we can comfortably generate private and public keys and either can be used for encryption and decryption.
It is also noticed that, by using one prime number and the one non negative integer, we have more choice for selecting a pair (p, q) and hence it takes more time to break the enhanced RSA by previous methods of cryptanalytic attacks [10].

5. PLAY COLOR CIPHER ALGORITHM:

Increased violence / adversary activities in recent times and a doubt about existing security algorithms [2] have created a need for inventing stronger secure algorithms rather then updating the existing one. For this purpose a stronger encryption algorithms using substitution and permutation got importance because they play vital role in many cryptographic algorithms. Most of the cryptographic algorithms are very familiar to the cryptanalysts and were even sharing braking techniques through hackers built in board; hence, we can say that, secrecy always depends on the key rather then algorithm. Another problem with the existing algorithm is that, many of them they work for either binary digits or alphanumeric characters but none of them fit for the combination of character, diagrams and images.

The challenge is to implement stronger and secure cryptographic algorithm which can encrypt/decrypt the information built with the characters, numbers, symbols, diagrams and images [3].

To meet this confronts, Udaya et al, have invented a new cryptographic algorithm and named it as 'Play Color Cipher (PCC-1)' in Feb 2010[11], initially they have considered an input built with only alphanumeric characters, and keyboard symbols. For encryption and decryption we have to give the starting address and increment value of the color and this number should be less then or equal to 256x256x256x256. The strength of this algorithm is, in the world of the computer we have 18 Decillions of colors and for substituting the colors in place of characters we can pick any of the color combination form the available massive number of colors, with this they have proven that this algorithm is resistant to birth day attack, meet in the middle attack and brute force attack. The main drawback in this algorithm is it doesn't consider diagrams and images for conversion.

In April 2011, Dr Vinaya et al, have updated the PCC-1 and named it as PCC-2[12], with 92 bit / 23 decimal numbers as a key, this key in turn divided in to three parts starting address(40dig), increment value(16dig) and key for transposition(36dig) based on Sub key generation algorithm. For the secure transmission of the key they have used RSA public key cryptography algorithm. PCC-2 built in three phases, initially the massage with alphanumeric characters, diagrams and images were converted in to RTF format, then a permutation is applied on the out put of phase one, permutation is based on the 9 digit decimal number, finally they have applied play color on the out put of phase two. Limitations noticed in this is, the key length is limited to 23 decimal / 92 bits binary and have only three stages.
In April 2011, Kallam et al, have reorganized the PCC-2 and named it as PCC-3[13]. In this they have considered multiple transpositions and substitutions with 128 binary/32decimal key to enhance the security of the algorithm. With this, if we perform one encryption per microsecond it takes $5.4X10^{24}$ years for brute force approach, hence it is cryptographically stronger.

Even though PCC-3 is more stronger, in June 2011 Udaya et al have enhance the PCC-3 by involving iterative and modular arithmetic functions in key generation algorithm and named it as PCC-4[14]. Because secrecy all ways depend on the key rather then algorithms in this they have mainly focused on strengthening key generation algorithm.

In Sep 2011, Kallam et al, have modernized PCC-4 by involving multiple transpositions and substitution with a large alphanumeric key and iterative functions, named it as Play color Cipher -5[15]. In this method they permitted alphanumeric key in 32 characters instead of only decimal number. By using sub key generation algorithms the key have been sub divided in to four parts. From the first two parts, 1to 15 and 16 to 22 characters, they have calculated the sum of ASCII values of all characters individually and named them as parameter1 as parameter2. The third part is 23^{rd} character. By calculating the sum of the digits in the ASCII values of 23^{rd} char, they picked up a particular predefined integral function. The out put of this function by passing parameter 1 and 2 is the starting address and the increment values for play color substitution. The last part of the sub key generation algorithm is from 24^{th} to 32 characters, from this the key for permutation have been generated. With, 32 alphanumeric characters as key, iterative functions and four rounds they have proven that the PCC-5 is very potential one.

In August 2011, Ravindra et al, have restructured the PCC-5 with five rounds including large alphanumeric key, modular arithmetic and integral functions and named it as PCC-6[16]. They have updated PCC-5, to exhibit a strong avalanche effect and proven that it cannot be broken by cryptanalytic attack.

6. CONCLUSION:

A Brief explanation on Importance of cryptography is given. Recent update on Playfair, poly alphabetic and RSA has been discussed. Mainly focused on the Play color cipher algorithm, a brief report on its six variations has been discussed.

7. ACKNOWLEDGMENTS:

The first like to thank the management and Principal of AZCET for providing all the resources and also like to thank the editor and review committee, IJMA for their valuable suggestions.

REFERENCES:

[1] Denning, D., F. Ayoub, "Cryptographic techniques and network security", IEEE proceedings, Vol 131, 684-694, Dec 1984.

[2] Stalling, " Cryptography and network security", Fourth edition, LPE, 81-7758-774-9.

[3] Ravindra babu, Udayakumar, "A Survey on Cryptography and Steganography Methods for Infromation Security", IJCA, 0975-8887, Vol 12, No-2, Nov2010.

[4] Ravindra, Udaya and Vinaya babu, An Improved Playfair Cipher Cryptographic Substitution Algorithm, JARCS, (0976-5697), Volume 2, No-1, Jan-Feb 2011.

[5] Ravindra, Udaya and Vinaya babu, An Extension to traditional Playfair Cipher Cryptographic Substitution Method, IJCA, (0975 – 8887), Volume 17, No-5, March 2011.

[6] Ravindra Babu, Udaya Kumar and Vinaya babu, An Enhanced Poly alphabetic Cipher using Extended Vigenere Table, IJARCS, (0976-5697), Volume 2, No.2, Mar-April 2011.

[7] Ravindra Babu, Udaya Kumar and Vinaya babu, An Enhanced and Efficient Cryptographic Substitution Method for Information Security, is communicated to IJMA, It is under review process.

[8] Ravindra, Udaya Kumar and Vinaya babu, A Contemporary Poly alphabetic Cipher using Comprehensive Vigenere Table, WCSIT,(2221-0741), Vol.1,No 4, 167-171,2011

[9] Alaa, Bilal, A fast approach for braking RSA cryptosystem, WCSIT,2221-0741,Vol 1,No 6, 260-263, 2011.

[10] Ravindra Babu, Udaya Kumar and Vinaya babu, An Enhanced RSA public key cryptographic algorithm, communicated to IJARCS, 0976-5697, In the press.

[11] Ravindra, Udaya and Vinaya babu, A Paper on "a block cipher generation using Color Substitution" is published in International Journal of Computer Applications (0975 – 8887), Volume 1- No-28, US, @2010.

[12] Ravindra Babu, Udaya Kumar and Vinaya babu, A New Frame Work for Scalable Secure Block Cipher Generation Using Color Substitution and Permutation on Characters, Numbers, Images and Diagrams, IJCA, Volume 20-no.5, April 2011.

[13] Ravindra Babu, Udaya Kumar and Vinaya babu, A More secure block cipher generation involving multiple transposition and substitution with a large key, IJARCS, (0976-5697), Vol 2, No 2, Mar-April 2011.

[14] Ravindra Babu, Udaya Kumar and Vinaya babu, A Modern Play color cipher involving dynamic permutated key with iterative and modular arithmetic functions, IJARCS, (0976-5697), Vol 2, No 3, May-June 2011.

[15] Ravindra Babu, Udaya Kumar and Vinaya babu, A Variable length block cipher generation using modern play color cipher algorithm with alphanumeric key and iterative functions, published in the proceedings of ICNICT-11, ISBN 978-93-81126-21-1, No 56, 288-293.

[16] Ravindra Babu, Udaya Kumar and Vinaya babu, An Unassailable Block Cipher generation with an extended play color cipher, concerning a large alphanumeric key, modular arithmetic and integral functions, (0975-8887),IJCA, Volume 28-no.9, August 2011.

****

