Data security using play color cipher substitution technique & Armstrong number

Sarang Deshpande[1], Maheep Tiwari[2], Deepak Singh[3]
[1, 2] Department of Computer Engineering
[1, 2] Mumbai University

Abstract- *In this paper a block cipher is developed with play color cipher algorithm and Armstrong number. In it a alphanumeric key is used with transposition and substitutions. This paper provides a technique to encrypt the data using a key involving Armstrong numbers and play color cipher as the password. The encryption, decryption, key generation is explained with suitable example. The cipher is very strong as it has double security by using play color cipher and Armstrong number*

Keywords- Armstrong numbers, data security, play color cipher, authentication and cryptography.

I. INTRODUCTION

Cryptography is the practice and study of techniques for secure communication in the presence of third parties called adversaries. More generally, cryptography is about constructing and analyzing protocols that prevent third parties or the public from reading private messages;[3] various aspects in information security such as data confidentiality, data integrity, authentication, and non-repudiation are central to modern cryptography. Modern cryptography exists at the intersection of the disciplines of mathematics, computer science, and electrical engineering.

In the present world scenario it is difficult to transmit data from one place to another with security. This is because hackers are becoming more powerful nowadays. To ensure secured data transmission there are several techniques being followed. In present paper we have used a 32 character alphanumeric key with UTF-8 to exhibit language independent cipher & proven that it is safe from known cryptanalytic attack. block cipher is developed with play color cipher algorithm. It also reduces the size of the plain text when it is encrypted in to cipher text by 4 times, without any loss of content. Cipher text occupies very less buffer space; hence transmitting through channel is very fast. With this the transportation cost through channel comes down.

The cipher is very strong as it is indicated by examining the cryptanalysis. Encryption and decryption require the use of some secret information, usually referred to as a key. The data to be encrypted is called as plain text. The encrypted data obtained as a result of encryption process is called as cipher text. Depending on the encryption mechanism used, the same key might be used for both encryption and decryption, while for other mechanisms.

II. PROPOSED ALGORITHM

All types of characters, numbers, and symbols converted into an UTF-8(Unified text format -8) character format. The plain text shown in figure is a combination of characters, numbers and special symbols is converted into cipher text and snap shot of which is shown.

Encryption:

1. Step1: select an alphanumeric key as plain text

ABCDabcd1234@#$*

2. Step2: plain text to UTF-8 format
   (ASCII values).
3. Step3: apply play color cipher on key
4. Step4: select any one color as a default color and enter color values for other two colors
5. Step5: Enter key value.
6. Step6: select file to encrypt.
7. Step7: select Armstrong number which assigned to key value and encrypt the file
8. Step8: File is encrypted.

Decryption:

1. Step1: Select file to decrypt.
2. Step2:Enter the key value.
3. Step3: Apply reverse play fair cipher.
4. Step4:Enter the key value received on mail.
5. Step5:Armstrong number will Automatically assigned to the key value.
6. Step6: File is decrypted.

Encryption

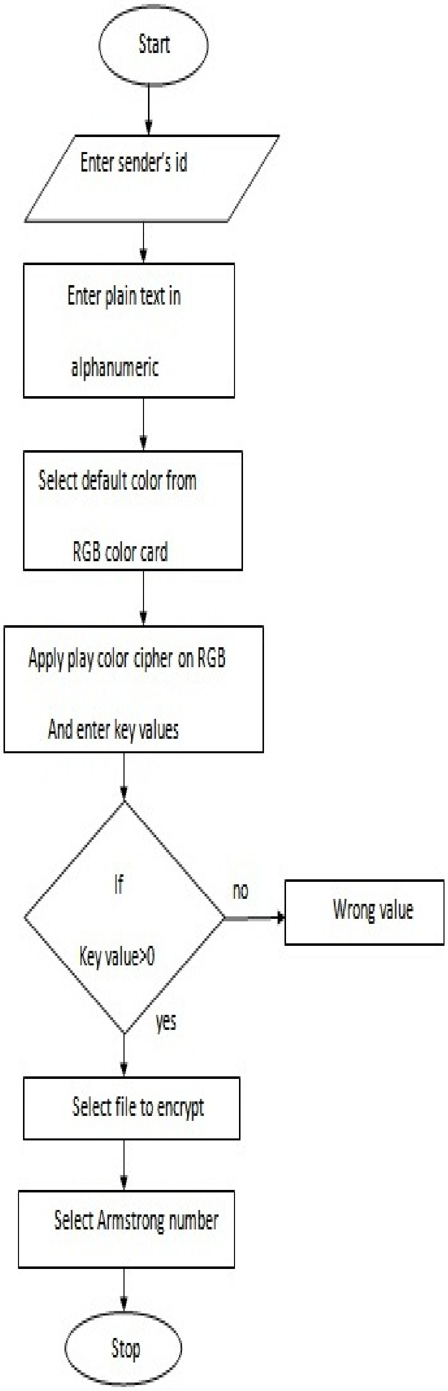

Start
Enter sender's id
Enter plain text in alphanumeric
Select default color from RGB color card
Apply play color cipher on RGB And enter key values
If Key value>0
no
Wrong value
yes
Select file to encrypt
Select Armstrong number
Stop

Figure 1. Encryption

Decryption

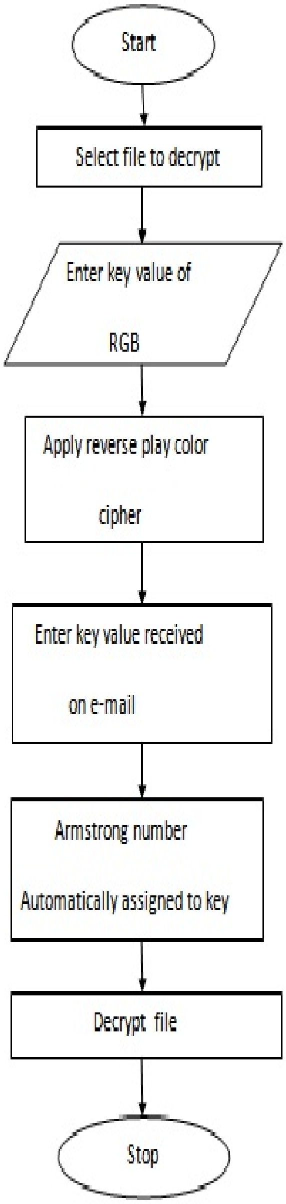

Start
Select file to decrypt
Enter key value of RGB
Apply reverse play color cipher
Enter key value received on e-mail
Armstrong number Automatically assigned to key
Decrypt file
Stop

Figure 2. Decryption

AES algorithm

Key Expansions—round keys are derived from the cipher key using Rijndael's key schedule. AES requires a separate 128-bit round key block for each round plus one more.

Initial Round- AddRoundKey—each byte of the state is combined with a block of the round key.

Rounds:

1. SubBytes—a non-linear substitution step where each byte is replaced with another according to a lookup table.

2. ShiftRows—a transposition step where the last three rows of the state are shifted cyclically a certain number of steps.
3. MixColumns—a mixing operation which operates on the columns of the state, combining the four bytes in each column.
4. AddRoundKey

Final round

1. SubBytes
2. ShiftRows
3. AddRoundKey.

Play fair cipher algorithm

The Play fair cipher uses a 5 by 5 table containing a key word or phrase. Memorization of the keyword and 4 simple rules was all that was required to create the 5 by 5 table and use the cipher.

To generate the key table, one would first fill in the spaces in the table with the letters of the keyword (dropping any duplicate letters), then fill the remaining spaces with the rest of the letters of the alphabet in order (usually omitting "Q" to reduce the alphabet to fit; other versions put both "I" and "J" in the same space). The key can be written in the top rows of the table, from left to right, or in some other pattern, such as a spiral beginning in the upper-left-hand corner and ending in the center. The keyword together with the conventions for filling in the 5 by 5 table constitute the cipher key.

Then apply the following 4 rules, in order, to each pair of letters in the plaintext:

1. If both letters are the same (or only one letter is left), add an "X" after the first letter. Encrypt the new pair and continue. Some variants of Play fair use "Q" instead of "X", but any letter, itself uncommon as a repeated pair, will do.
2. If the letters appear on the same row of your table, replace them with the letters to their immediate right respectively (wrapping around to the left side of the row if a letter in the original pair was on the right side of the row).
3. If the letters appear on the same column of your table, replace them with the letters immediately below respectively (wrapping around to the top side of the column if a letter in the original pair was on the bottom side of the column).
4. If the letters are not on the same row or column, replace them with the letters on the same row respectively but at the other pair of corners of the rectangle defined by the original pair. The order is important – the first letter of the encrypted pair is the one that lies on the same row as the first letter of the plaintext pair.

To decrypt, use the INVERSE (opposite) of the last 3 rules, and the 1st as-is (dropping any extra "X"s, or "Q"s that do not make sense in the final message when finished).

There are several minor variations of the original Play fair cipher.

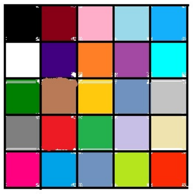


Figure 3.

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

Figure 4.

Conversion of plain text to UTF-8

All types of characters, numbers, and symbols Converted into an UTF-8(Unified text format8) Character format. The plain text shown in step1 is a combination of characters, numbers and special symbols is converted into cipher text.

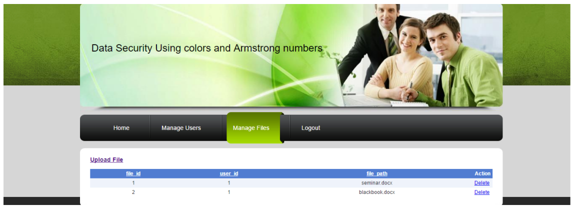
Character matrix

Utf-8 characters are changed into a matrix in square form. These characters are useful for any known language of the world. Here we are using Only English language character set.

Color matrix

From the character matrix by using key K1 and its ASCII value, key K2 for increment of color with its ASCII value a color matrix in created

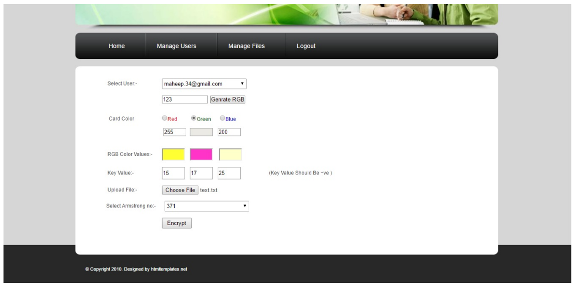
III. IMPLEMENTATION



Upload File

file_id	user_id	file_path	Action
1	1	seminar.docx	Delete
2	1	blackbook.docx	Delete

Figure 5.



Select User:- maheep.34@gmail.com

123 Genrate RGB

Card Color ○Red ●Green ○Blue

255 200

RGB Color Values:-

Key Value:- 15 17 25 (Key Value Should Be +ve)

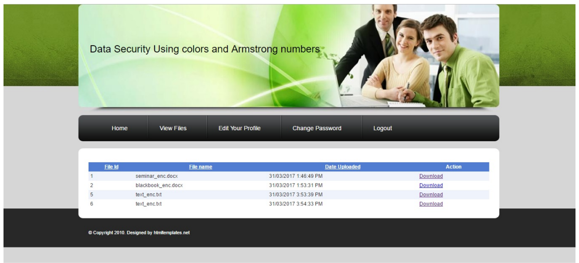
Upload File:- Choose File text.txt

Select Armstrong no:- 371

Encrypt

© Copyright 2010. Designed by htmltemplates.net

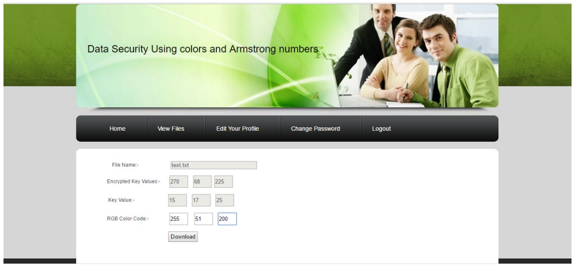
Figure 6.



File Id	File name	Date Uploaded	Action
1	seminar_enc.docx	31/03/2017 1:46:49 PM	Download
2	blackbook_enc.docx	31/03/2017 1:53:31 PM	Download
5	text_enc.txt	31/03/2017 3:53:39 PM	Download
6	text_enc.txt	31/03/2017 3:54:33 PM	Download

© Copyright 2010. Designed by htmltemplates.net

Figure 7.



File Name:- text.txt

Encrypted Key Values:- 270 68 225

Key Value:- 15 17 25

RGB Color Code:- 255 51 200

Download

Figure 8.

IV. CONCLUSION

The above combination of secret key and public key cryptography can be applied mainly in military where data security is given more importance. This technique provides more security with increase in key length of the Armstrong numbers. Thus usage of three set of keys namely colors, additional set of key values and Armstrong numbers in this technique ensures that the data is transmitted securely and accessed only by authorized people.

REFERENCES

[1] https://www.shoretel.com/ web - communication - cryptography - and-network -security

[2] https://www.pearsonhighered.com/product/Stallings - Instructor - Solutions-Manual-for-Cryptography- and-Network - Security- Principles-and-Practice-6th-Edition /9780133354744.html.

[3] https://www.pearsonhighered.com/product/Stallings-Instructor - Solutions-Manual-for-Cryptography-and-Network-Security-Principles-and-Practice-6th-Edition/9780133354744.html.

[4] http://whatis.techtarget.com/definition/RGB-red-green-and-blue.

[5] https://decisionstats.com/2013/12/14/play-color-cipher-and-visual-cryptography/