An Unassailable Block Cipher Generation with an Extended PCC, Concerning a Large Alphanumeric Kay, Modular Arithmetic and Integral Functions

Prof. Ravindra Babu Kallam
Research Scholar, JNTUH
VITS SET, Karimnagar
A.P, India

Dr. S.Udaya Kumar
Principal
M.V.S.R Engineering College
Hyderabad, A. P, India

Dr. A.Vinaya Babu
Director, Admissions
J.N.T.U.H, Hyderabad
A.P, India

ABSTRACT
In this investigation, we have developed an unbreakable block cipher with extended play color cipher algorithm. This includes multiple transpositions, substitutions, modular arithmetic, integral functions and a 32 characters alphanumeric key. These functions mutate the plain text in various ways before it takes the shape of cipher text. The process of encryption, decryption and the sub key generation method were explained with example. The avalanche effect and the cryptanalysis examined in this analysis clearly indicate that the cipher is very strong one.

General Terms
Crypt analysis, Block cipher, Play color cipher, Encryption, Decryption, Decillions, Security and Algorithm.

Keywords
Symmetric block cipher, Cryptanalysis, Play color cipher (PCC), Substitution, Permutation, RSA algorithm, Rich text format (RTF), PUB: Public key of user B, PRA: Private Key of user A, PUA: Public key of user A, PRB: Private key of user B.

1. INTRODUCTION
A number of cryptographic algorithms [1][2][3] have been developed and updated in the recent past, which can be found in the literature. In a current investigation, Udaya et al. have developed a modern cryptographic algorithm in three variations, by name it is Play Color Cipher [4][5][6][7][8].The variations are PCC-92, PCC-128 and PCC-32AN, the first two version are based on 92, 128 binary keys and the third one uses 32characters alphanumeric key. In these algorithms they have also involved number of permutation, substitution, iterative and modular arithmetic functions to strengthen the cipher.

In the present paper we have updated PCC-32AN, to exhibit a strong avalanche effect and proven that it cannot be broken by cryptanalytic attack.

2. KEY SELECTION & DISTRIBUTION
In this we have used a 32 characters alphanumeric key. The key format and Steps involved in sub key generation algorithm is shown in the figure 1 and 6. Procedure for transferring key from source to the destination is shown in the Figure 2.

- Select key 'K', should be 32 alphanumeric characters, for our convenience from know on the word "alphanumeric characters" will be called as a "characters" in this paper.
- In the above 32 characters: from LHS to RHS, the sub key generation algorithm considers out put of the first 15 characters as parameter 1 (K1), next 7 characters as parameter 2 (K2), the out put of 23rd characters (K3) will be used to select integral function and the out put of last 9 characters (K4) will be used as a key for transposition
- K1 and K2 will be passed as a parameters to the function selected by K3 and the output will be the starting address K1' and Increment value K2', for selecting color in play color cipher algorithm.
- There is one more key K5 will be generated by the sub key generation algorithm based on the length of the plaintext, used for transposition in the process of encryption and decryption.

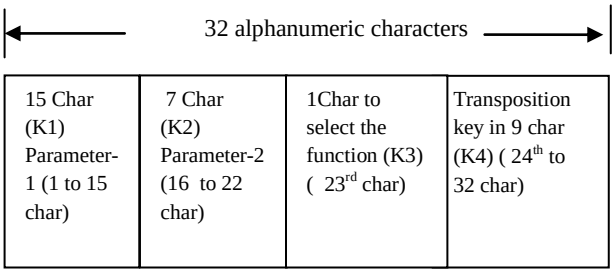

Figure 1: Key format in 32 alphanumeric characters

- Use RSA [9] Public key encryption algorithm for key distribution as shown in Figure 2:
- Encrypt K using senders (Source A) private key (PRa) for authentication ---------- 2.1
- Encrypt the result of 2.1 using receivers (User B) public key (PUb) for confidentiality. ---------- 2.2
- Send the result of 2.2 to the receiver----------2.3
- Decrypt 2.3 by using PRb ---------- 2.4
- Decrypt 2.4 by using PUa ---------- 2.5

Hence with the both authentication and confidentiality we have distributed the keys between User A and User B.

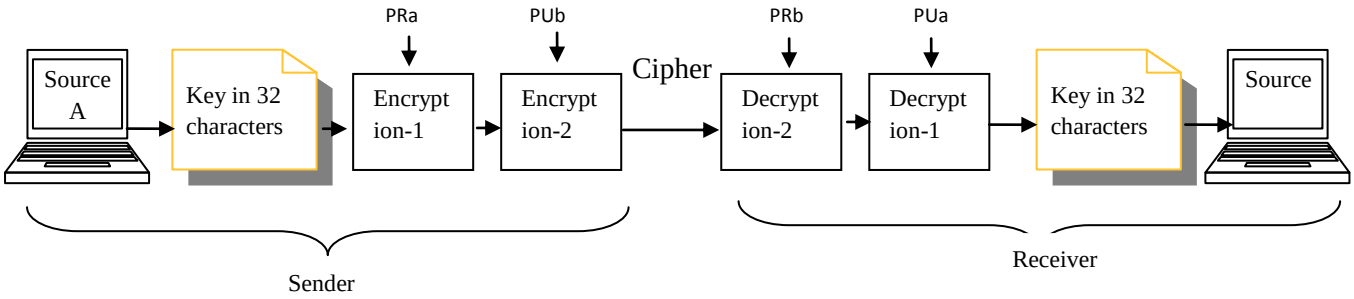

Figure 2: Secure Transmission of Key using RSA

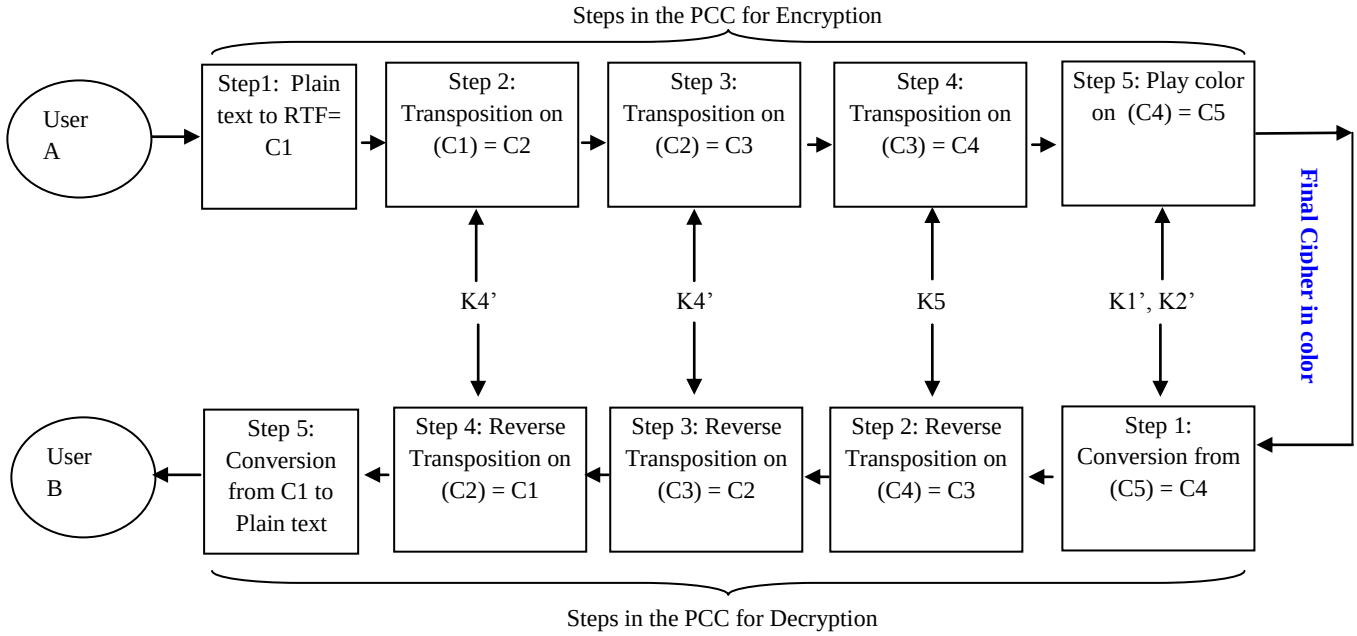

Figure 3: Process of Encryption & Decryption using Play Color Cipher

3. DEVELOPMENT OF THE CIPHER

In this we have considered a block of plain in the form of alphanumeric characters, symbols, images and diagrams, etc as shown in the figure 4.

PCC TESTING FOR AVALANCE EFFECT
TEXT CAN BE ANY CHARACTERS,
DIAGRAMS AMD IMAGES
1111%%%%%&&&999999__+++++++

Figure 4: Plain text 1 considered for encryption

For the development of the cipher we have five phases in this algorithm as shown in the figure 3. To exhibit and prove a strong avalanche effect we have considered another plain text in which we have changed a single character in the first plain text as shown figure 5. It is to be noted that only the first character in the plain text is differ in figure 4 & 5, which is character P is changed to Q. A desirable property of any encryption algorithm is that a small change in either the key or the plain text should produce a significant change in the cipher.

QCC TESTING FOR AVALANCE EFFECT
TEXT CAN BE ANY CHARACTERS,
DIAGRAMS AMD IMAGES
1111%%%%%&&&999999__+++++++

Figure 5: Plain text 2 considered for encryption

In particular, a change in one bit / character of the plain text or key should produce a change in many bits / characters of the cipher text. The same we have proven in fourth and fifth phase of the PCC.

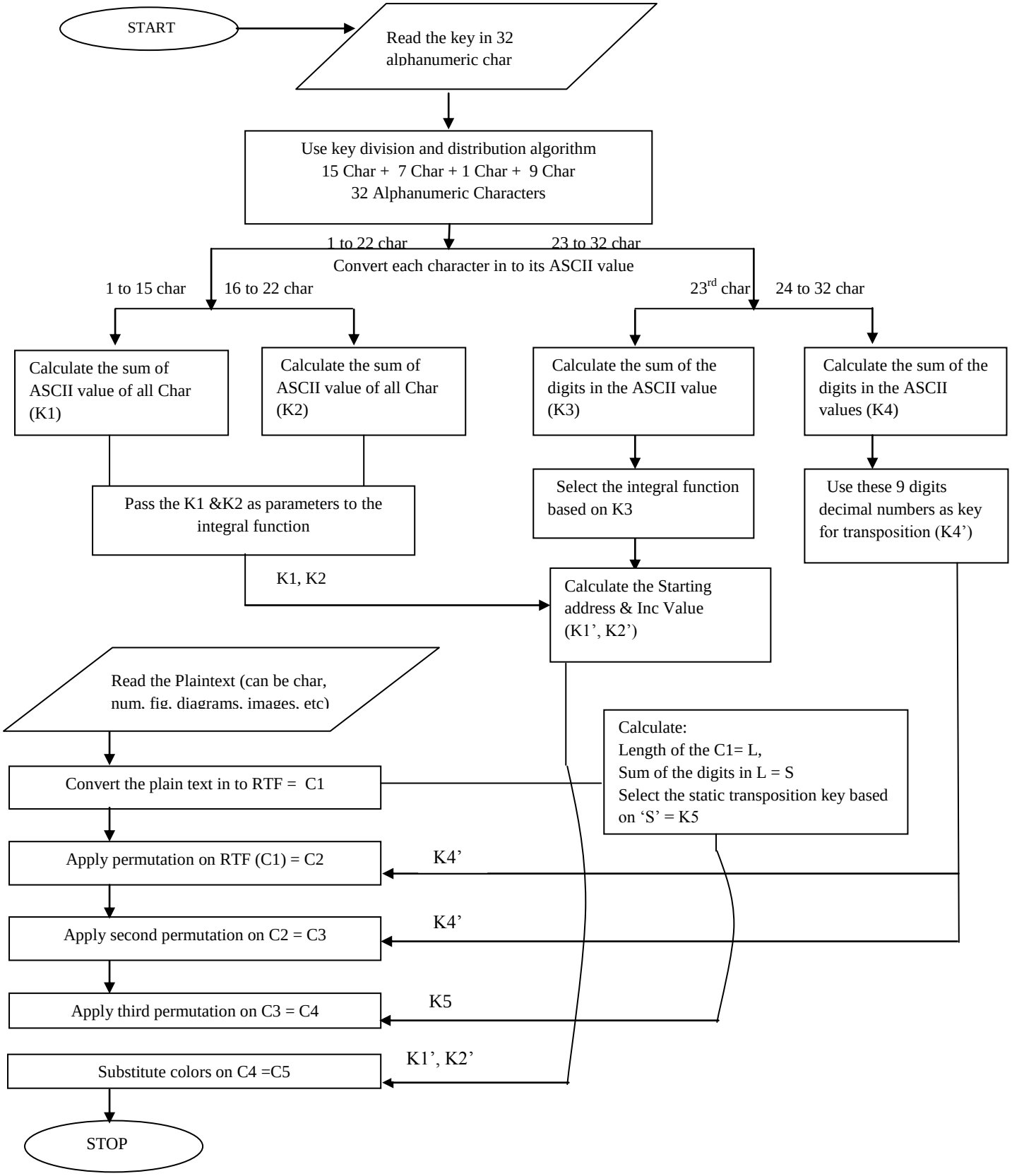

Figure 6: Flow chart for encryption process

{\rtf1\ansi\ansicpg1252\deff0\deflang1033{\fonttbl{\f0\fswiss\fprq2\fcharset0 Microsoft SansSerif;}{\f1\fnil\fcharset0 Microsoft Sans Serif;}}\viewkind4\uc1\pard\nowidctlpar\f0\fs20 QCC TESTING FOR AVALANCE EFFECT\parTEXT CANBEANYCHARACTERS,\parDIAGRAMSAMDIMAGES\par1111%%%%&&&999999__+++++++\par\pard\f1\ fs20{\pict\wmetafile8\picw762\pich658\picwgoal436\pichgoal376010009000003f022000000005111000506060607090806070907060608 0b08090a0a0a0a0a06080b0c0b0a0c090a0a0affdb00430102020202020202050303050a0706070a0a0a0a0a 0a0a0a0a0a0a0a0a0a0a0a0a0a0a0a0a0a0a0a0a0a0a0a0a0a0a0a0a0a0a0a0a0a0a0a0a0a0a0a0a0a0a0a0a0a0affc0001108003 900420301220002110103110 1ffc4001f000001050101010101010000000000000000010203040506070809 0a0bffc400b52433627282090a161718191a25262728292a3435363738393a434445464748494a535455565758595a636465666768696a737475767778797a838485868788898a92939495969798999aa2a3a4a5a6a7a8a9aab2b3b4b5b6b7b8b9bac2c3c4c5c6c7c8c9cad2d3d4d5d6d7d8d9dae1e2e3e4e5e6e7e8e9eaf1f2f3f4f5f6f7f8f9faffc4001f0100030101010101010101000000000000000102030405060708090a0bffc400b5110002010204040304070504040001027700010203110405213106124151076171132232810814429 1a1b1c109233352f0156272d10a162434e125f11718191a262728292a35363738393a434445464748

Figure 7: a snap shot of converted Cipher text in Rich text format C1, out of 18 pages of out put

\1tfrna{\isan\pcsid\522feg1lfde\naf0\{330ofg1\{blt0fntsswisf\\fcf2\qahprM t0ecirs tofsaSroirSe;fnsf\f1\in}{rachfesl\rcMi sot0na St sof};ifr}Sekwievni\\1uc\apd4iwno\cdrdf\arp\0tlCQ0 2 CfsGNTISF TELAAV NAOREFEF TCCraXE\pB ANCETAHCYARAN,RSEp\CTAIDarDMASIAMp\ESGraMA%1111%%99&&&99%%++_+_++99rpa\\++1fd\rf\paip{ \0tcs2faetmli\wwcpi\67e86hicp852\ogcwila\pci\p6gh43637l02177000210013001205413105124101063171122761810844321ba111c2953332f209276251d0126340a1f251714e2a9112618a22985372387333936544436 4a4498445a476555475356a955635866576467a966736877765874782a87837978865884892a989389799658949a2aa9a3997aa658a430fd120000101f30010031523c81ef98ccad9bb4fac800ae4e9960393e630d2365357d7e83228670f919e93b79d6164b4827acb3529f6304 dc502c8ea382bef4ff8cf04a4cdbea583c4f8e8777dfaae46dbb5178bf384ab2a898c9e0a673784f20f62ec27d53f6c3c895ba6 e35cb5c54efe8acad64596d2f2b5d34b67b3d5ffcbd4a1091603527192e38f0ecb38fb54402e63d3508f0bdf34ef65eb5358664d46c330bc32f0937bbacb4d2211000faf0f97facc9abd736b5913211e1549a19754axvsnbagsntu2udsf34,oip7abda0c2cb3n

Figure 8: a snap shot of first transposition C1 to C2 out of 18 pages of out put

tfra{n\sian\cspi\d522egf1flde\afn0{\330fgo1{\bltfn0tsswis\\fffc2\qhparMt0eircstofsSraoriSefn;s\ff1\n}i{archfsle\crMiots 0anStsoifr}Sewkievin\1\uc\pda4wino\drcd\farp0t\lQC2CfsNGTISFEALAVAONRFEEFCCTETraE\XpBANCETHACY RAAN,RSE\CpTIADGaRrMDASAIM\pESGaMrA1%111%%99&&&9%9%++_+_+9+9rpa\+\+f1d\r\pfapi{\0cst2afetm i\lwcwpi\7e68h6icp528\gocwia\lpic\p6h4g36o534a958447565585556463a6955867669666757437a6797877a787868548 378a998828ee3a8eae99b51a1d544dadcebf520a8bcbc3eca0cd6ad860547bb218cdb213eccd603ee0134fd0409d5238277ab f6781af71024f56eae55397e2d73de50e575220e20fba50fde2b1ea4bc9c153e9574ab7d0ac2c38b7f639149dfa127be21a658 9c567088ff2fbac80990c712f3c4ed3a373541e18d7601fc356e4374f1670926ddefce34a7fceb6ec5523df0c0bab1d9f5c76e7 8d7d6a23d3d7be10839f51fe201c15f749ae1a875b1a1c3a7d92d9f923d19a10c9890767cdfe4d8df9fb2ee383867ff537a865 81a1ac8634fe692a348d07b915c06f04df32b13d759e2e57971b86b0eb396a1f2359f7e1e594bbaf2142e8e77df9c95facbdfa 72def401eef6f7b0b62ab571637062a0f6d004b518c80f44eeb1c1f89ee653e95517a8df58d4044ad3f43a644f1b0bf56db781

Figure 9: a snap shot of Second transposition C2 to C3 out of 18 pages of out put

rn\a{\tf1\picsians2fdeg152\\nlaf0def0o\fg133{t0\fntbl{sfs\\fwisqachpr2\fecMirst0 sa Srooft ;ifnsSer\ifn}{f1\fersl\cha srot0Mict nsof Sar}}Seif;vnki\iew\a\pd4uc1\cidrdnowp\f0tlar\2 CCfs0 QSFGETINLAORAVATECCEEFFaXTE\prC BETANYAARANCHEp\CTRS,RAGarDISIDAMMGrpaMAES\1%%%111&999%%&&9_+++99_++\\++parrf1\pad\f0 tics2{\pmlfi\weta\6w7e8picp8652\ichiloa\pcwg6gch43\pilaaa0a00a0000a0aa0aaaa0a00a0000a0aa0aaaa0a00a0c011ff000 020480390000003122131021000c4111fff1000100000010510110001001000000000003200001000070450 69fbf800a0928898a365999499a9a97899365a2aa4aabaaa78a9365b2bb4bbcbab78b9365c2cc4ccdcac78c9352dd4dddd9d67d8143eaee2 eeee8e56e7a32f9ef1ffff7f45f694fc8ffaf100000f0111103001000011011000100000001000000365020040000a07809f50bb fc400001110024430200400004075041770002010300102411310052105106241123276711841432108111c29a1b2f5209 333512d0162713240a617114e25f12261891a85a372292333936738365 4a4444454a4784947653555556635895a576646667736896a587747767788379a82587848868899389a925879499699aa399aa2587a4aa6abb2a9aa476b3bb5bbcc2b89ba47

Figure 10: a snap shot of third transposition C3 to C4 out of 18 pages of out put

rnki\iew\a{\tf1\picsians2fdeg15bvfrdshkut2y\u\unlajfk0ldmesfd0oc\nfmgs13w3s{ft0h\jfknltbl{sfs\\fwisqachpr2\fecMirst
0saSrooft;ifnsSer\ifn}{f1\fersl\chasrot0Mictnsofr}}Seif;n\a{\tf1\picsia\iew\a\pd4uscd1f\gchijdkrldnowp\f0tlar\2CCfs0SF
GTIENTNVLAAORVEFCEFEFaXATF\pCrBETANYAARANCHEp\CTRS,RAGarISIDMMGrpaMAES\1%%%111&
999%%&&9_+++99_++\\++parrf1\pad\f0tics2{\pmlfi\weta\6w7e8picp8652\ichiloa\pcwg6gch43\pilaaa0a001e59e3e5e6
9851df87a5434adf04d4134fba6467bdb8f50ac138a5f1ad0651a7cb7780dec3bf352b12d86fdadd8901b9256742a5f0c8259
3744e733fef378fc72f673a8fac35b10bb0f0956bf6bb0a668c9a98ab7b71ee48249bdefd39e74dccd0649faa38c76ed5f255d3
be2b0ecab0294af159eb2252ffe9ed6cfaff141a6b345a103b34ac79577adbede782ea272c4bdb980df9c15851fb9f17d0bde8
7eccc5f1f89ea123c4cbc4c8f088deb67243243fab0ea76fdc2ad89f0ea9619c3e83a6be1e33570baed6344ed79bf19ac3c9395
47e6bb83def9cbe537fc7319628a21fea72484e54fa0c1eeac632b3fdf49e4f002af7f7fa79ef123979eebbcdaf42b1f1448b7c1
c6d9f19eb2ed257fbf8d5d6d873b4e996a9b1fb5f2dcf110aff6fcb4d95012fd781e8fb11d00770bf30f4acf11fec3f5df64f07e8
8e3b484b1601b89f935e611c556b156f986fc8facb1b620f279c65a193aebffebc3b510866cf737774c5effe3e20727caaaeffc2
73f0025c559f7fec69dd961e73b6c12be3c3be881b1966f383bc541bf2d8aff54f4e0758f2a8e8df84351e00c2758cec7f18a4f
56af33e37a323bef7d47e4c86f5b3006aef502ef009ff3fb7d72486fa2579f7b08fe4270f0fdc9f6c1dd0b3e25e524951e4f1d0d
15923db7851b679e3a0961ebb9e2f7135f9b54bae2e2e8714fcfd95af97adb72edfce64eff01f6bbhm7i8ygrfthio6xsderhytda

Figure 11: a snap shot of third transposition C3 to C4 out of 18 pages of out put after changing one character in the plain text input (figure 5)

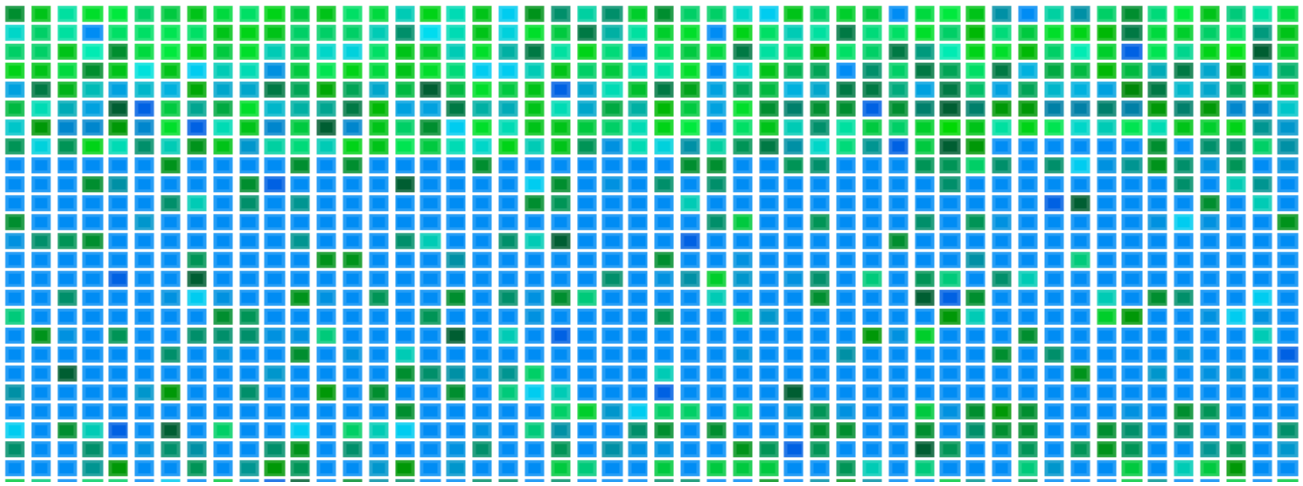

Figure 12: a snap shot of color substitution on C4 to produce final cipher C5 using play color cipher

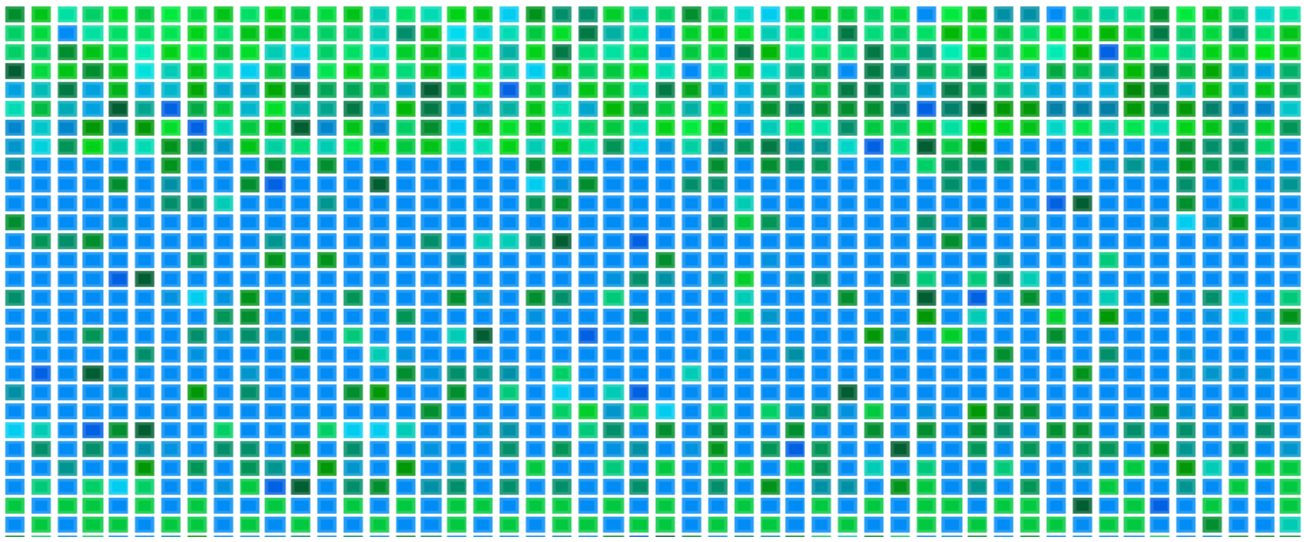

Figure 13: a snap shot of color substitution on C4 to produce final cipher C5 using play color cipher After change a single character in the plain text input (figure 5)

3.1 Converting Plain text in to the RTF format:

We can renovate all types of characters, numbers, symbols, diagrams and images by using rich text box in to Rich text format. By using this facility the plain text is converted in to an unintelligible text.

The plain text considered is shown in figure 4, which is the combination of alphanumeric characters, symbols, diagrams and images. We can observe that the entire plain text is comfortably converted in to cipher text and a snap shot of the output is shown in the figure 7 and named it as Cipher text C1.

3.2 First permutation on the output of previous step (3.1)

Transposition is nothing but the changing the order of the characters in the text, so that the out put spells differently and not easily intelligible. For performing permutation write the text in the rectangle, row by row, and read the message off, column by column, but permute the order of the columns. The order of the columns then becomes key to the algorithm.

Many transposition algorithms they don't allow the decimal number in the transposition key to repeat, but in our sub key generation algorithm we have a provision of this. To enhance the strength of the cipher C1, we have performed transposition on it by using a key K4'. This key is generated from the last 9 characters of the main key and is a 9 digit decimal number. In the example shown it is " 339789789". A snapshot of the out put in this stage is shown in the figure 8, and named it as C2.

3.3 Second transposition on the output of preceding step (3.2)

To strengthen the cipher in the previous step 3.2 we did the transposition on the C1 once again with the same key K4'. With multiple permutations, we can enhance the strength of the cipher, so that it is not easily brittle. This can be repeated number of times based on the requirement; it is recommended that to use different keys for each permutation to develop stronger cipher. For our expediency we have used a common key and the result is shown in the figure 9, named it as Cipher C3.

3.4 Third permutation on the output of previous step (3.3)

To make the cipher more potential and to give the avalanche effect, we did the permutation on the preceding step 3.3 with a new key K5, which is derived from the length of the cipher text C1. It is noticeable that the length of the cipher texts C1, C2 and C3 are same. The out put of this stage is shown in the figure 10 and named it as Cipher C4.

3.5 Applying play color cipher on the out put of prior step (3.4) using K1'and K2'

With our Play Color Cipher[4] each Character (Capital, Small letters, any kind of text, Numbers (0-9), Symbols) in the plain text is substituted with a color block from a 18 decillions of colors[5] available in the computer world. In this we have considered only ARGB with the maximum number of 255 X 255 X 255 X 255 = 4228250625 colors, to make the cipher stronger.

For color substitution we have used two keys K1'and K2', Which are derived from the first 22 characters of the main key.

In the example shown the value of the starting address K1' is'20964' and the Increment value K2' is ' 315', by applying this on the out put Cipher(C4) in previous step, we got the color code as shown in the figure 12. This is the final cipher C5 generated by the source anticipated for receiver.

4. CRYPTANALYSIS

The cryptanalyst attacks which are normally considered in the literature of Cryptography are

1. Cipher text only attach (Brute force attack)
2. Known plaintext attack
3. Chosen plaintext attack
4. Chosen cipher text attack

In this paper the key 'K' allows of 32 alphanumeric characters. From the Left hand side first 22 characters (15 + 7) are used to calculate the starting address and increment value for color substitution, next characters (23^{rd}) is used for selecting integral function and the remaining 9 characters (24^{th} to 32 positions) are used as a key for transposition. In this we have three possibilities:--

Case 1 key can be only characters: Because, the alphabets are only 26, to enter 32 characters in the key, obviously some characters will have to be repeated. In these circumstances:

Maximum number of Keys = $(26)^{32} = 1.9 \text{ X } 10^{45}$ Keys

If the time required for the determination of the plain text for one value of the key in the key space is taken as 10^{-3} seconds, then the time required for obtaining the plain text by considering all the possible keys in the key space is $1.9X10^{45}X10^{-3}$

If we perform one encryption per micro second it takes

$$\frac{1.9 \text{ X } 10^{45} \text{ X } 10^{-3}}{365 \text{ X } 24 \text{ X } 60 \text{ X } 60} = 6 \text{ X } 10^{35} \text{ Years}$$

Case 2: out of 32 characters first 26 can be characters and the remaining 6 can be numbers between '0 to 9'. In this situation:

Maximum number of Keys = $(26)^{26} + (10)^6 = 6 \text{ X } 10^{36}$ Keys. If we perform one encryption per micro second it takes

$$\frac{6 \text{ X } 10^{36} \text{ X } 10^{-3}}{365 \text{ X } 24 \text{ X } 60 \text{ X } 60} = 1.9 \text{ X } 10^{27} \text{ Years}$$

Case 3: key can be only numbers: Because the key length is 32 and the numbers can be any decimal number between '0 to 9', naturally the numbers will be repeated in the key. In this condition:

Maximum number of keys= $(10)^{32}$.

If we perform one encryption per microsecond it takes:

$$\frac{10^{32} \text{ X } 10^{-3}}{365 \text{ X } 24 \text{ X } 60 \text{ X } 60} = 3.1 \text{ X } 10^{29} \text{ Years}$$

In all three cases the number of possible keys were large, and the time required to try all probable keys is too high. Brut force attack is not possible and hence; it is impossible to break the cipher.

In the case of known plain text attack, we have to know as many pairs of plaintext and cipher text as we require. The number of colors in the computer world is more then 18 Decillions, with minor difference we have thousands of shades in the same color, by looking at the colors it is impossible to obtain the plain text, even if you have number of plain text and the corresponding cipher text, moreover the input to the color substitution algorithm is not the actual plain text rather it was permuted twice in the process. With permutations and substitutions in different stages we can conclude that knowing plain text does not work. In the last two cases of the cryptanalysis attack, no scope is found for breaking the cipher.

Other then all these, to prove that the cipher is potential one, it is mandatory that the cipher should confirm a strong avalanche. To reveal and confirm a strong avalanche effect we have considered another plain text in which we have changed a single character in the first plain text as explained in section 3 and it is shown figure 5. It is identifiable that the only first character in the plain text is differed in figure 4 & 5. We have also encrypted the new plain text with the same key 'K', with the same procedure and experimentally noticed that there is more then 90% of the cipher in the second experiment is differ from the first experiment. A snap shot of the third transposition and the color substitution of both the experiments were shown in the figures 10, 11, 12 and 13.

In view of the above conversation, we bring to a close that the Cipher is a very strong.

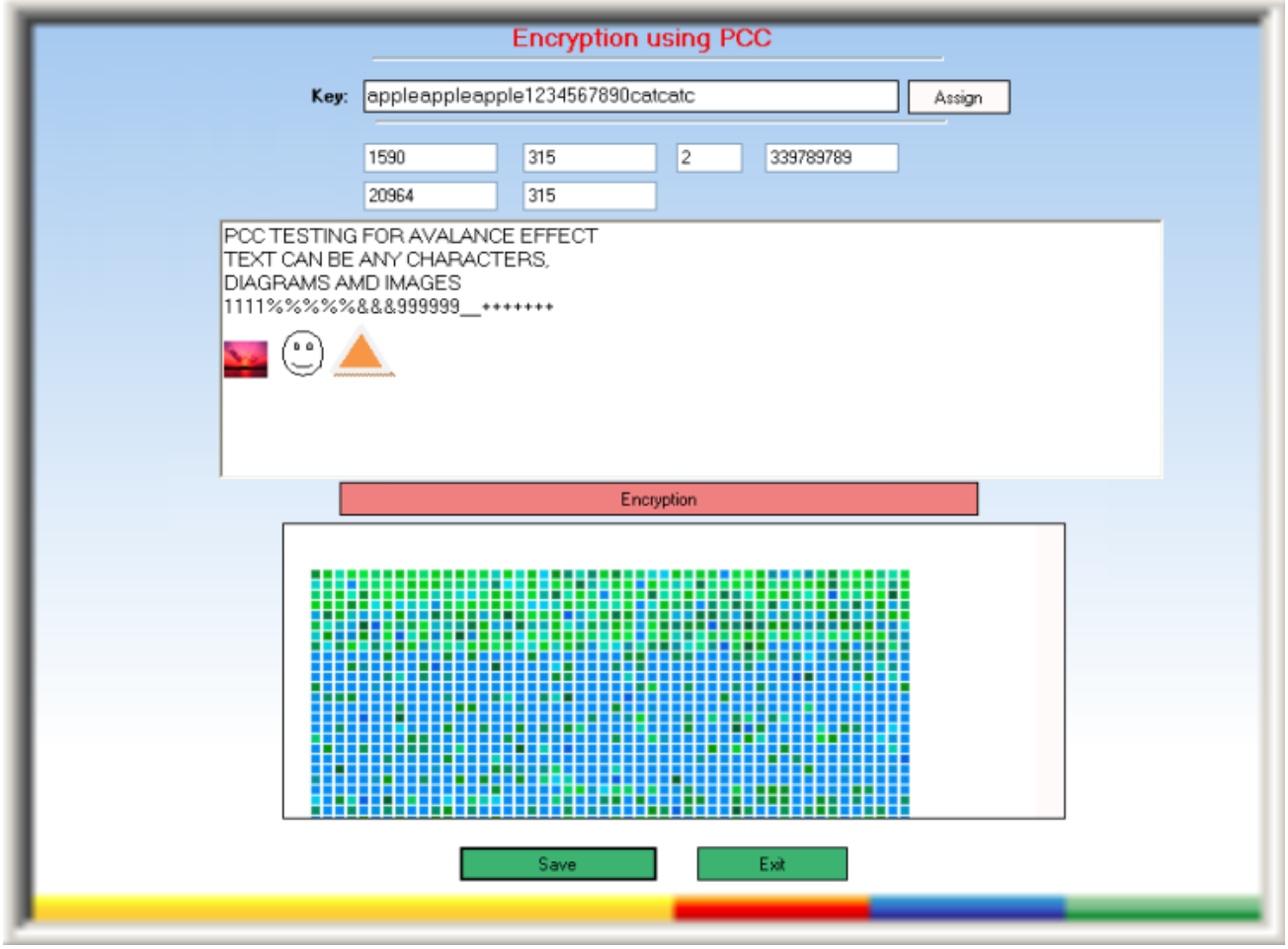

Figure 13: Encryption using extended PCC with 32 alphanumeric key

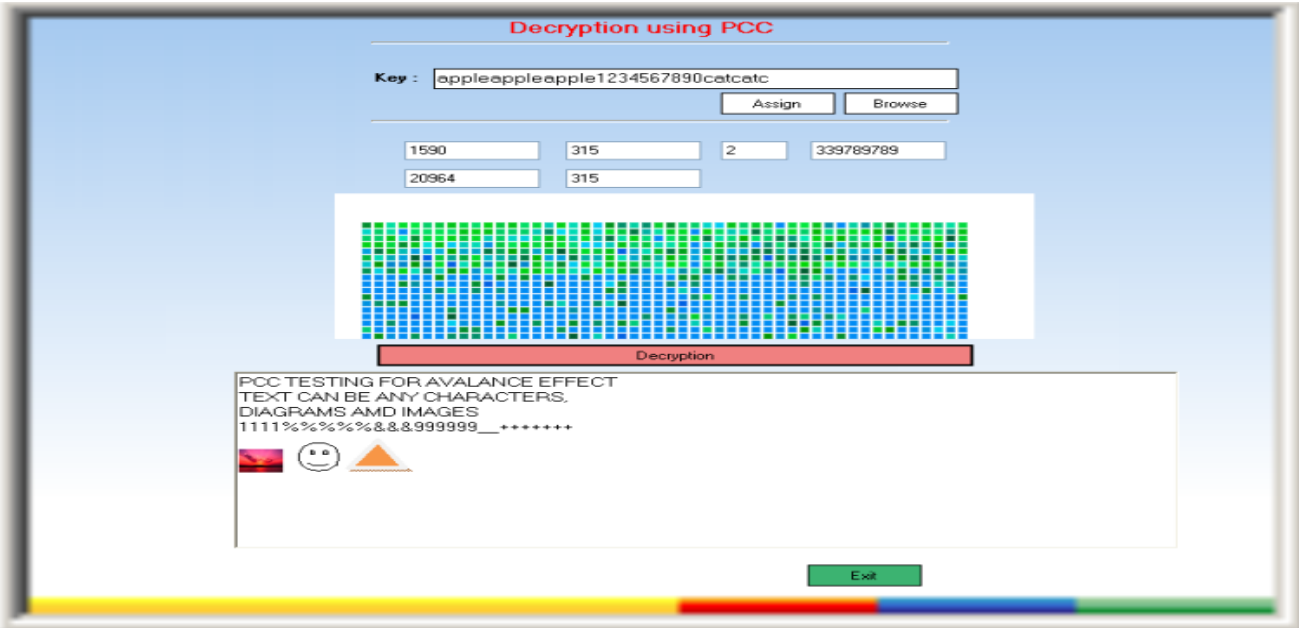

Figure 14: Decryption using extended PCC with 32 alphanumeric key

5. RESULTS

The invented play color cipher algorithm works with 32 alphanumeric key and it is confirmed that it is comfortably converting all kinds of text, symbols, diagrams and images as shown in the figure 13 and 14. The process of conversion with examples was explained. The strength of the any algorithm depends on key rather then the algorithm, in this the length of the key is 32 characters and proven that it is far from crypt analysis attacks and especially it gives a strong avalanche effect.

6. CONCLUSION

In this paper we have developed an extended play color cipher algorithm i.e. a symmetric key encryption algorithm using multiple transformation and color substitution. In this we have involved 32 alphanumeric characters as a dynamically permuted key with integral functions. We have proven that it can encrypt / decrypt all kinds of text, numbers, symbols, images and diagrams with example as shown in figure 13 and 14. For performing one encryption per micro second it takes minimum 1.9×10^{27} years.

For transferring key from sender to receiver we have used RSA algorithm and the procedure was explained with neat diagram. Specially we have concentrated on the sub key generation algorithm, explained the three possible cases and its time complexity. The brief explanation and the advantages of RTF were given; production of cipher text in five phases was explained with example.

Lastly, we conclude that, with the 32 characters alphanumeric key, the cipher is very strong and the algorithm is potential one.

7. ACKNOWLEDGMENTS

The first author likes to thank Dr. A. Vinaya Babu and Dr. S. Udaya kumar for their valuable advices and supervision round the clock to complete the task fruitfully.

He also likes to thank Management of AZCET and VITS SET for providing all the facilities. Special thanks to IJCA for allowing us to use its template.

8. REFERENCES

[1] Ravindra Babu K, Dr. S. Udaya Kumar, A Survey on Cryptography and Steganography Methods for Information Security, IJCA, Volume-12, No-2, November 2010

[2] Ravindra Babu K, Dr. Udaya kumar, Dr. A.Vinaya Babu, An Improved Playfair Cipher Cryptographic Substitution Algorithm, IJARCS, Volume 2, No-1, Jan-Feb 2011.

[3] Ravindra Babu K, Dr. Udaya Kumar, A contemporary poly alphabetic cipher using comprehensive vigenere table, WCSIT, Vol 1, No 4, 167-171, 2011.

[4] Lt. Ravindra Babu Kallam, Dr. S.Udaya Kumar, A Block Cipher generation using Color Substitution, IJCA, 2010 Vol 1, No-28.

[5] Ravindra Babu K, Dr. S.Udaya Kumar, Dr.A.Vinaya Babu, A new frame work for scalable secure block cipher generation using color substitution and permutation on characters, numbers, images and diagrams, IJCA, Vol 20.No 5,April 2011.

[6] Ravindra Babu K, Dr. S.Udaya Kumar, Dr.A.Vinaya Babu, A more secure block cipher generation involving multiple transposition and substitution with a large key, IJARCS, Vol 2, Mar-April 2011.

[7] Ravindra Babu K, Dr. S.Udaya Kumar, Dr.A.Vinaya Babu, A modern PCC involving dynamic permuted key with iterative and modular arithmetic functions, IJARCS,Vol 2, No 3, May-June 2011

[8] Ravindra Babu K, Dr. S.Udaya Kumar, Dr.A.Vinaya Babu, A variable length block cipher generation using modern PCC algorithm with alphanumeric key and iterative functions, accepted for the conference ICNICT-11, Sep 2011.

[9] William Stallings, Cryptography and Network Security, Principles and practice, 5th edition, 2008.