International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2018 IJSRCSEIT | Volume 3 | Issue 1 | ISSN : 2456-3307

Advance Cryptography Using Color Substitution

Komal Chavan, Ashwini Patil, Dipali Patil, Anup Mourya
Information Technology Department, RGIT, Mumbai, Maharashtra, India

ABSTRACT

The emerging threats to information security are increasing at an alarming rate. The most influential and universal approach to counter such threats is encryption. Traditional encryption techniques use substitution and transposition. Substitution techniques map plaintext into ciphertext. In all traditional substitution techniques, characters, numbers and special symbols are substituted with other characters, numbers and special symbols. In this paper, an innovative cryptographic substitution method is proposed to generate a stronger cipher than the existing substitution algorithms. This method emphasizes on the substitution of characters, numbers and special symbols with color blocks. This algorithm of substitution is based on Play Color Cipher. The cryptanalysis done on this will prove that the cipher is strong.

Keywords: Play Color Cipher (PCC), Color Substitution, Color Block, Color Code.
General Term: Encryption, Decryption, Block Cipher, Play Color Cipher, Security and Algorithm.

I. INTRODUCTION

Overview:

Information Security which refers to protecting information in potentially hostile environments is a crucial factor in the growth of information-based processes in industry, business, and administration. Cryptography is a key technology for achieving information security in communications, computer systems, electronic commerce, and in the emerging information society. The security of cipher text is completely dependent on two things: the power of the cryptographic algorithm and the confidentiality of the key. Intruder activities in recent times have created a need for inventing stronger and more secure algorithms. In recent past many researchers have modified the existing algorithms to fulfill the need in the current market, yet the ciphers are vulnerable to attacks.

Problem definition:

RSA is very vulnerable to chosen plaintext attacks. There is also a new timing attack that can be used to break many implementations of RSA. The RSA algorithm is believed to be safe when used properly, but one must be very careful when using it to avoid these attacks. A well-known attack on RSA can break the RSA in 953 milliseconds of length „n" with 180 digits, where n is the product of two unequal prime numbers.

One of the most extensively used cryptographic method, DES, was also broken and announced by electronic Frontier Foundation in July 1986. A newly discovered technique known as biclique cryptanalysis helps attackers to remove about two bits from 128-, 192-, and 256-bit keys and recover AES secret keys up to five times faster than previously possible.

Substitution techniques like Caesar Cipher, Mono alphabetic Cipher, play fair Cipher and Poly Alphabetic Ciphers are not strong enough since they are vulnerable to brute-force attacks.

Scope of project:

Each character (available on the keyboard) in the plaintext is substituted with a color block from the available 18 Decillions of colors in the world and at the receiving end the cipher text block (in color) is decrypted in to plain text block. It is resistant against problems like Meet in the middle attack, Birthday attack and Brute force attacks.

The size of the plain text is also reduced by 4 times when it is encrypted, in a lossless manner. The space occupied by the cipher text in the buffer is very less; hence transmitting through a channel is very fast which subsequently brings down the transportation cost. Relevance and Motivation of project the aim of this project is to provide secure communication between two parties. So, that secret message/data cannot be compromise. The objective for developing this project is that, it can provide the security of data. It will also provide the transfer of data from one machine to another. Only the authorized user and administrator can access the application. The emerging threats to information security are increasing at an alarming rate. The most influential and universal approach to counter such threats is encryption. Traditional encryption techniques use substitution and transposition. Substitution techniques map plaintext into ciphertext. In all traditional substitution techniques, characters, numbers and special symbols are substituted with other characters, numbers and special symbols. In this paper, an innovative cryptographic substitution method is proposed to generate a stronger cipher than the existing substitution algorithms. This method emphasizes on the substitution of characters, numbers and special symbols with color blocks. This algorithm of substitution is based on Play Color Cipher. The cryptanalysis done on this will prove that the cipher is strong.

1. Existing Cryptographic Systems:

In Symmetric-key ciphers, the sender sends the plaintext which is encrypted using a shared secret key. The receiver decrypts it using the same shared key. These ciphers consist of Substitution and Transposition ciphers. A Substitution cipher replaces one symbol with another. A Transposition cipher re-orders the symbols.

2.Modern Symmetric-Key Ciphers:

A symmetric-key modern block cipher encrypts an n-bit block of plaintext and decrypts n-bit block of ciphertext using a k-bit key. DES and AES are examples of this type of cryptography algorithm. Modern Stream Ciphers process the message bit by bit (as a stream) and typically have a (pseudo) random stream key.

3. Asymmetric-Key Cryptography:

This system is based on personal secrecy. Unlike symmetric key cryptography, this has distinctive keys: a public key and a private key. Public key of the receiver is used for encryption while the private key of sender is used for decryption. RSA is the most commonly used asymmetric key algorithm. The security of RSA relies on the difficulty of factoring large integers.

II. PLANNING AND FORMULATION

System Development Life Cycle:

The System Development Life Cycle is the process of developing information systems through investigation, analysis, design, implementation, and maintenance. The System Development Life Cycle (SDLC) is also known as Information Systems Development or Application Development.

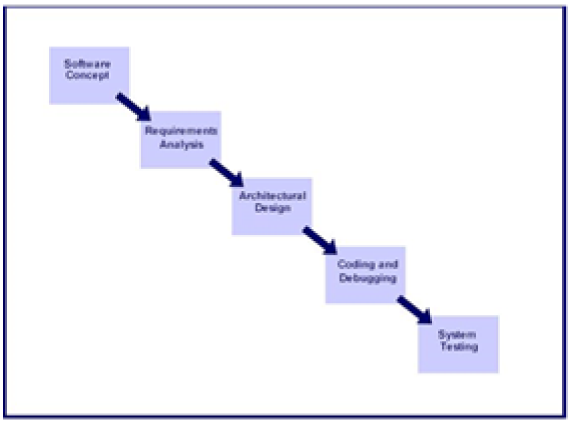


Figure 1. SDLC Diagram

Steps involved in the System Development Life Cycle: Below are the steps involved in the System Development Life Cycle. Each phase within the overall cycle may be made up of several steps.

Step 1: Software Concept:

The first step is to identify a need for the new system. This will include determining whether a business problem or opportunity exists, conducting a feasibility study to determine if the proposed solution is cost effective, and developing a project plan.

This process may involve end users who come up with an idea for improving their work. Ideally, the process occurs in tandem with a review of the organization's strategic plan to ensure that IT is being used to help the organization achieve its strategic objectives. Management may need to approve concept ideas before any money is budgeted for its development.

Step 2: Requirements Analysis:

Requirements analysis is the process of analyzing the information needs of the end users, the organizational environment, and any system presently being used, developing the functional requirements of a system that can meet the needs of the users. Also, the requirements should be recorded in a document, email, user interface storyboard, executable prototype, or some other form. The requirements documentation should be referred to throughout the rest of the system development process to ensure the developing project aligns with user needs and requirements.Professionals must involve end users in this process to ensure that the new system will function adequately and meets their needs and expectations.

Step 3: Architectural Design:

After the requirements have been determined, the necessary specifications for the hardware, software, people, and data resources, and the information products that will satisfy the functional requirements of the proposed system can be determined. The design will serve as a blueprint for the system and helps detect problems before these errors or problems are built into the final system. Professionals create the system design, but must review their work with the users to ensure the design meets users' needs.

Step 4: Coding and Debugging:

Coding and debugging is the act of creating the final system. This step is done by software developer.

Step 5: System Testing:

The system must be tested to evaluate its actual functionality in relation to expected or intended functionality. Some other issues to consider during this stage would be converting old data into the new system and training employees to use the new system. End users will be key in determining whether the developed system meets the intended requirements, and the extent to which the system is actually used.

Step 6: Maintenance:

Inevitably the system will need maintenance. Software will definitely undergo change once it is delivered to the customer. There are many reasons for the change. Change could happen because of some unexpected input values into the system. In addition, the changes in the system could directly affect the software operations. The software should be developed to accommodate changes that could happen during the post implementation period.

There are various software process models like: -

- ✓ Prototyping Model
- ✓ RAD Model
- ✓ The Spiral Model
- ✓ The Waterfall Model
- ✓ The Iterative Model

Of all these process models, we’ve used the Iterative model (The Linear Sequential Model) for the development of our project.

III. METHOLODOGY

a) Proposed System:

We propose a cryptographic substitution method called Color coded cryptography which modifies the “Play Color Cipher”. This is a symmetrical system which is implemented by encryption of text by converting it into colors. Each character of the message is encrypted into a block of color. Every character will be substituted by a different color block. The inverse process is used to produce the original text from colors at the receiver side. The user enters a message which is the plaintext. A channel needs to be chosen from the three-color channels i.e. red, green and blue (RGB). The user must specify the values for the R, G and B channels from the range 0-255. Also, a block size needs to be specified. All the characters of the text are then converted to blocks of color formed by combining the values of R, G and B channels. A single image is then generated for all the color blocks of the message. The block size and the channel selected form the symmetric key.

b) Proposed Methodology:

1) **Encryption:**

1.Accept the input text file and the key.
2.Separate the input text into individual characters.
3.Input the block size, color-channel (R/G/B) and a color (RGB value).
4.Depending on the block-size (say n), divide the picture box into a grid of blocks, each of size n.
5.Add the ASCII value of every character with its position and put the value in the color-channel selected.
6.For the remaining 2 channels, put the value of the Color inputted by the user.
7.Draw the bitmap image.
8.Generate the Key.
9.Send the image to the receiver.

2) **Decryption:**

1. Add the ASCII value of every character with its position and put the value in the color-channel selected.
2. For the remaining 2 channels, put the value of the Color inputted by the user.
3.Draw the bitmap image.
4.Generate the Key.
5.Send the image to the receiver.
6.Subtract the blocks position from that value.
7.Convert the resulting value into character and get the text.
8.Decrypt the text using the decryption process of the standard encryption algorithm used.
9. Get the original text back.

IV. SYSTEM REQUIREMENTS

Hardware Requirements:

- System: Pentium IV 2.4 GHz.
- Hard Disk: 40 GB.
- Floppy Drive: 1.44 Mb.
- Monitor: 14’ Color Monitor.
- Mouse: Optical Mouse.
- Ram: 512 Mb.
- Keyboard: 101 Keyboard.

Software Requirements:

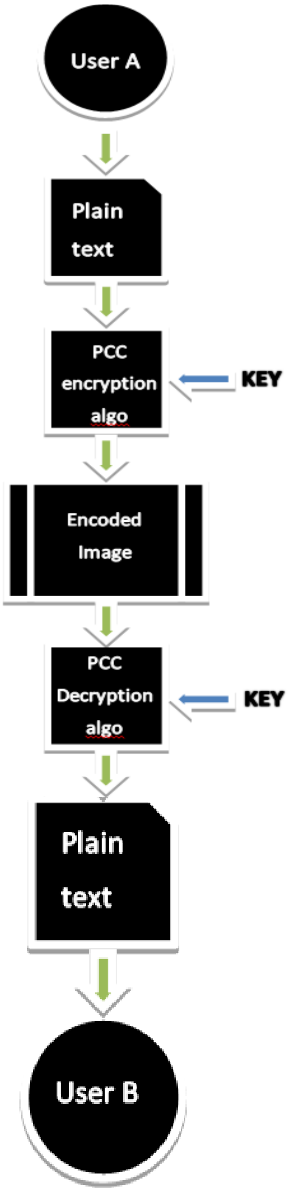
- Operating system: Windows XP.
- Coding Language: C#.Net
- Data Base: SQL Server 2008.

V. TECHNOLOGY USED

C#.net C# is an elegant and type-safe object-oriented language that enables developers to build a variety of secure and robust applications that run on the .NET Framework. You can use C# to create Windows client applications, XML Web services, distributed components, client-server applications, database applications, and much, much more. C# syntax is highly expressive, yet it is also simple and easy to learn. The curly-brace syntax of C# will be instantly recognizable to anyone familiar with C, C++ or Java.

VI. APPLICATION

This system of color cryptography can be used for authentication of login systems. During the registration process, the new user will enter his personal details and the password. The password is then encrypted into a color-coded image using the proposed color substitution algorithm. The image is then stored at the server. At the time of login, the user enters the username and password. Based on the username, corresponding image of the password is retrieved from server, decrypted and converted to text. This text is then matched with the password entered by the user. If it matches, the user successfully logs in. The key for encryption and decryption can be based on the parameters of the personal details entered by the user. Mathematical functions performed on the timestamp of registration and user's date of birth can generate a key. Thus, the need for storage of key is eliminated.



VII. CONCLUSION

Today's standard cryptographic methods are subject to a variety of attacks. An innovative approach presented and implemented in this paper makes information secure by color substitution. In future, the figures, tables, images, etc can be included in the plaintext for conversion and hence the scope of the algorithm can be increased

Literature Cited

•Advanced Cryptography Using Color Code Based Substitution with multi-language support/ (Monica Kanchan, Avinash Shaha, Jayesh Gupta, Sunita Naik)/International Journal of Computer Application (0975-8887)

•National Bureau of Standards "Data Encryption Standard" FIPS-PUB, 46, Washington, D.C., Jan 1977.

•Johan Hastad, 1986. "On using RSA with low exponent in a public key network", Advances in Cryptology CRYPTO ‟85, LNCS 218, pp. 403-408.

VIII. ACKNOWLEDGMENTS

We wish to express our sincere gratitude to Dr. U. V. Bhosle, Principal and Prof. D. M. Dalgade, H.O.D of Information Technology Department of RGIT for providing us an opportunity to do our project work on "Color cryptography using substitution method". This project bears on imprint of many people. We sincerely thank our project guide Prof. S. K. Sabnis for his guidance and encouragement in successful completion of our project synopsis. We would also like to thank our staff members for their help in carrying out this project.

IX. REFERENCES

[1]. Prof. R.M.Sahu, Akshay Godase, Pramod CONTROL ENGINEERING, Vol. 4.

[2]. Kanchan Mahajan, Proff.J.S.Chitode, "Waste Bin Monitoring