iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 7 **Issue:** V **Month of publication:** May 2019

DOI: https://doi.org/10.22214/ijraset.2019.5331

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.177
Volume 7 Issue V, May 2019- Available at www.ijraset.com

Advance Cryptography using Color Blocks

[1]Dimpal Ramanuj, [2]Chandresh Parekh, [3]Kaushal Bhavsar
[1]PG Student, [2]Asst Professor, [3]Phd research scholar
[1]Mtech Cyber Security, Raksha Shakti University, Ahmedabad, Gujarat

Abstract: ***In the world of emerging technology, cryptography is used in Authentication/Digital Signatures, Time Stamping, Electronic Money, Secure Network Communications (Secure Socket Layer (SSL), Kerberos), Anonymous Remailers, Disk Encryption etc. In past years cryptology has evolved from secret art to modern science. Weaker algorithms and algorithms with short keys are disappearing, political controls of cryptography have been reduced, and secure cryptography is becoming more and more a commodity. Moreover, implementations are becoming more secure as well. Since, information processing by electronic devices leads to a multitude of security relevant challenges, we need to keep evolving new cryptographic methods or algorithms day by day. This paper is about the new cryptographic development and how to use it to get a more secure communication over networks.***

Index Terms: Cryptography, color block, AES, Rail Fence, Flowchart, substitution, color conversion.

I. INTRODUCTION

There are many aspects to security and many applications, ranging from secure commerce and payments to private communications and protecting health care information. One essential aspect for secure communications is that of cryptography. But it is important to note that while cryptography is necessary for secure communications, it is not by itself sufficient.

Cryptography or cryptology (from Ancient Greek: κρυπτός, translit. kryptós "hidden, secret"; and γράφειν graphein, "to write", or -λογία -logia, "study", respectively) 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; 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, electrical engineering, communication science, and physics. Applications of cryptography include electronic commerce, chip-based payment cards, digital currencies, computer passwords, and military communications.[1]

Cryptography prior to the modern age was effectively synonymous with encryption, the conversion of information from a readable state to apparent nonsense. The originator of an encrypted message shares the decoding technique only with intended recipients to preclude access from adversaries. The cryptography literature often uses the names Alice ("A") for the sender, Bob ("B") for the intended recipient, and Eve ("eavesdropper") for the adversary. Since the development of rotor cipher machines in World War I and the advent of computers in World War II, the methods used to carry out cryptology have become increasingly complex and its application more widespread. Modern cryptography is heavily based on mathematical theory and computer science practice; cryptographic algorithms are designed around computational hardness assumptions, making such algorithms hard to break in practice by any adversary. It is theoretically possible to break such a system, but it is infeasible to do so by any known practical means. These schemes are therefore termed computationally secure; theoretical advances, e.g., improvements in integer factorization algorithms, and faster computing technology require these solutions to be continually adapted. There exist information-theoretically secure schemes that provably cannot be broken even with unlimited computing power—an example is the one-time pad—but these schemes are more difficult to use in practice than the best theoretically breakable but computationally secure mechanisms.[1]In This paper we have tried to develop a new algorithm with the combinations of different cryptographic methods and then converted the last output into colored blocks. We have presented an idea of the whole environment and process using the flowchart.

II. CHALLENGE OF CRYPTOGRAPHY

A. Cryptanalysis

It is an art of deciphering the cipher text without knowing the key or encryption. Some of the methods related to this are as follows

1) Cipher text Only: In this type of attack an attacker can access only cipher text or decrypted data but cannot access plain text. This type of attack is done on simple cipher like Caesar cipher where frequency analysis can be used to break the code.

2) Known Plain text: In this type a cryptanalyst has plaintext and their corresponding cipher text. Attacker tries to find out the relation between these two.
3) Chosen Cipher text: The attacker obtains the various plaintext corresponding to an arbitrary set of cipher text.
4) Chosen Plain text: The attacker obtains the various cipher text corresponding to an arbitrary set of plain text.
5) Adaptive Chosen Plain text: This is similar with the Chosen Plaintext, except in this attacker chooses subsequent set of plain text which is based on the information obtain from previous encryption methods.
6) Adaptive Chosen Cipher text: This is similar with the Chosen Cipher text, except in this attacker chooses subsequent set of cipher text which is based on the information obtain from previous encryption methods.
7) Related Key Attack: Like the chosen plaintext, attack in which attacker can obtain only cipher text encrypted with the help of two keys. These keys are unknown but the relationship between these keys is known. Example two keys differ by a single bit.

There are several issues related to cryptographic algorithm such as space complexity, time complexity and its resistance to various types of attacks. In order to implement an effective cryptographic algorithm all these aspects need to be considered in order to make it robust. Let's discuss these issues: -

a) *Time Complexity:* It is the amount of time required to encrypt and decrypt the data. The algorithm should be designed in such a way that it should take as less time as possible for its execution. Time complexity plays an important role in modern cryptography as more and more systems are working in a real time environment nowadays. Hence while implementing a cryptographic algorithm it is necessary to consider its time complexity.
b) *Space Complexity:* It is the amount of space consumed by cipher text as compared with plain text. As more and more mobile devices with limited connectivity in terms of data rate are being used nowadays, it is very essential to keep the size of cipher text being produced as small as possible as to deal with variable data rates. Thus, it is very important to device a way to reduce the size of cipher text as much as possible to increase data transmission efficiency.
c) *Security:* The very purpose of cryptography is to secure the data being transmitted over the network from various types of attacks. The data being transmitted is always vulnerable to various types of attacks such as men in the middle attack, brute force attack etc. Thus, in order to prevent the data from being compromised it is necessary to protect the data from unauthorized users. The feasibility of cryptography must be tested against such attacks so as to secure the data being sent. Hence providing security is one of the major issues of cryptography

III. ENCRYPTION IN YOUR DAILY LIFE

A. SSL Certificates

Browsing the internet is an activity that most of us do every day. On the internet, encryption comes in the form of Secure Sockets Layers (SSL) certificates. SSL protection is a security technology feature that website owners can buy in order to increase the security of their site.

You can recognize an encryption protected website from the green padlock and the "HTTPS" in the URL.

SSL protection establishes an encrypted communication channel between a browser and a web server.

An active SSL certificate on a web server is especially useful on websites where visitors enter sensitive information such as credit card information, phone numbers, IDs, etc. That means that all the data that is being transferred between a browser and a web server is encrypted for security and privacy reasons.

B. Cash Withdrawal from ATMs

Banks use Hardware Security Module (HSM) encryption methods in order to protect your PIN and other banking information while the transaction is in transit in the network.

HSM encryption comes in many different types but, in essence, it's function is to encrypt the 4 to 6 digit PIN of every person that uses the ATM. Then, the PIN is decrypted at the HSM side in order to execute and validate the transaction or money withdrawal.

This encryption method ensures that hackers won't be able to get their hands on your PIN in case they intercept the network data in transit.

C. Email

Webmail applications such as Gmail and Hotmail provide the earlier explained SSL encryption (HTTPS) in order to protect the user. However, it's important to note that SSL encryption does not encrypt the text in emails.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.177
Volume 7 Issue V, May 2019- Available at www.ijraset.com

Thus, without going too deep into the technical jibber-jabber, the NSA for example, would still be able to intercept your emails in readable text format.

Privacy-minded users are increasingly more often leaning towards end-to-end encryption email providers such as Proton mail and Counter Mail. Millions of users have already made the switch to similar encryption protected email providers.

This email software ensures that every sent and received email is encrypted into ciphertext. So, even when the email is intercepted, it's unreadable to anyone without the decryption key.

D. File Storage

Popular file storage platforms such as Dropbox and Google Drive, with 500 million and 800 million users respectively, greatly emphasize on the security of the platform.

Obviously, the platform wouldn't be used by millions of users – individuals and businesses – if it didn't provide a secure environment to store important files, photos and videos.

That means that every file is encrypted into cipher data in order to protect the users. Dropbox even stated in their security protocol that they break every piece of data into multiple other pieces and encrypt these smaller pieces of data one by one.

Both platforms protect files in transit between servers and apps, but also at rest (when it's stored on their server). Which is incredibly helpful for all these millions of users, to be sure all their important data is safely stored online.

E. Messenger Apps (WhatsApp)

According to TechCrunch, the popular messenger application WhatsApp had 1.5 billion active monthly users in Q4, 2017. Which is good for 60 billion messages sent per day.

It comes to no surprise that WhatsApp values the privacy of its users, which is why WhatsApp implemented complete end-to-end encryption in their messenger application. That means that all your messages, photos, videos, voice messages and files are secured.

Only the person you're communicating with is able to read what you're sending. End-to-end encryption also means that even WhatsApp is not able to read any messages, because it's stored on their server in encrypted format.

And the best thing is that WhatsApp automatically encrypts every message by default and there's no way to turn off the encryption.[2]

IV. METHODOLOGY

Using cryptographic algorithms applied on a set of input and then converting the obtained cipher text into colour block, a system is developed which need input of plain text and a pin. At this moment no validation is put on any of the input. The pin is to be used at the time of reversing the output of color block to plain text at the time of deciphering. Basic programming language is also used in this research work. And website is developed for demo of the work.

A. Algorithms Used

1) *Transposition of Rail Fence Cipher:* The rail fence cipher (also called a zigzag cipher) is a form of transposition cipher. It derives its name from the way in which it is encoded. In the rail fence cipher, the plain text is written downwards and diagonally on successive "rails" of an imaginary fence, then moving up when the bottom rail is reached. When the top rail is reached, the message is written downwards again until the whole plaintext is written out. The message is then read off in rows.
2) *Substitution:* In this process characters are converted to ascii character and then they are reverse.
3) *AES Encryption/Decryption:* The more popular and widely adopted symmetric encryption algorithm likely to be encountered nowadays is the Advanced Encryption Standard (AES). It is found at least six time faster than triple DES. A replacement for DES was needed as its key size was too small. With increasing computing power, it was considered vulnerable against exhaustive key search attack. Triple DES was designed to overcome this drawback but it was found slow.

The features of AES are as follows −

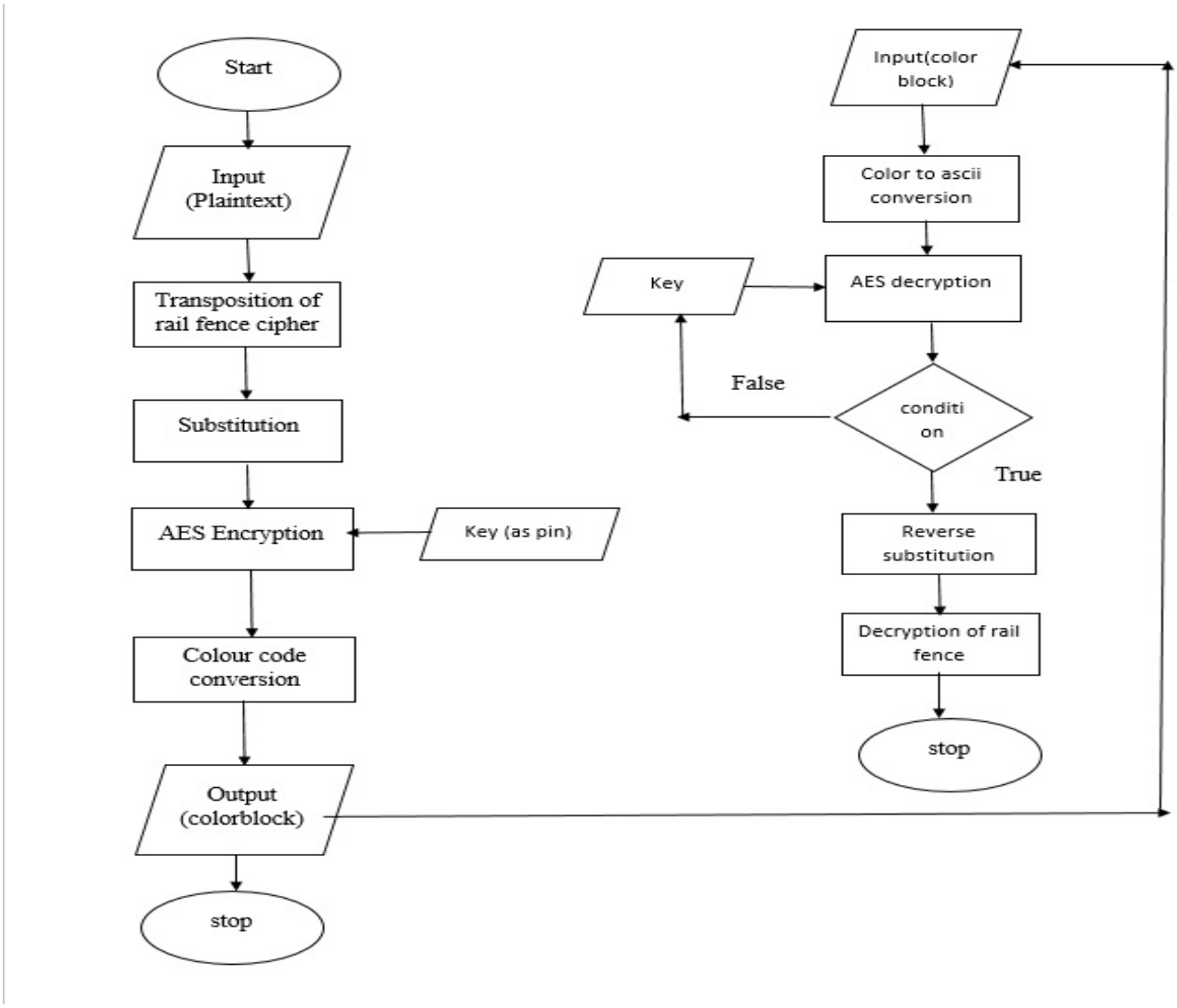
a) Symmetric key symmetric block cipher
b) 128-bit data, 128/192/256-bit keys
c) Stronger and faster than Triple-DES
d) Provide full specification and design details
e) Software implementable in C and Java

4) Operation of AES: AES is based on 'substitution–permutation network'. It comprises of a series of linked operations, some of which involve replacing inputs by specific outputs (substitutions) and others involve shuffling bits around (permutations). Interestingly, AES performs all its computations on bytes rather than bits. Hence, AES treats the 128 bits of a plaintext block as 16 bytes. These 16 bytes are arranged in four columns and four rows for processing as a matrix. The number of rounds in AES is variable and depends on the length of the key. AES uses 10 rounds for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys. Each of these rounds uses a different 128-bit round key, which is calculated from the original AES key.
5) *Colour Code Conversion:* The final input to this block is converted in color blocks.

B. Programming Languages Used

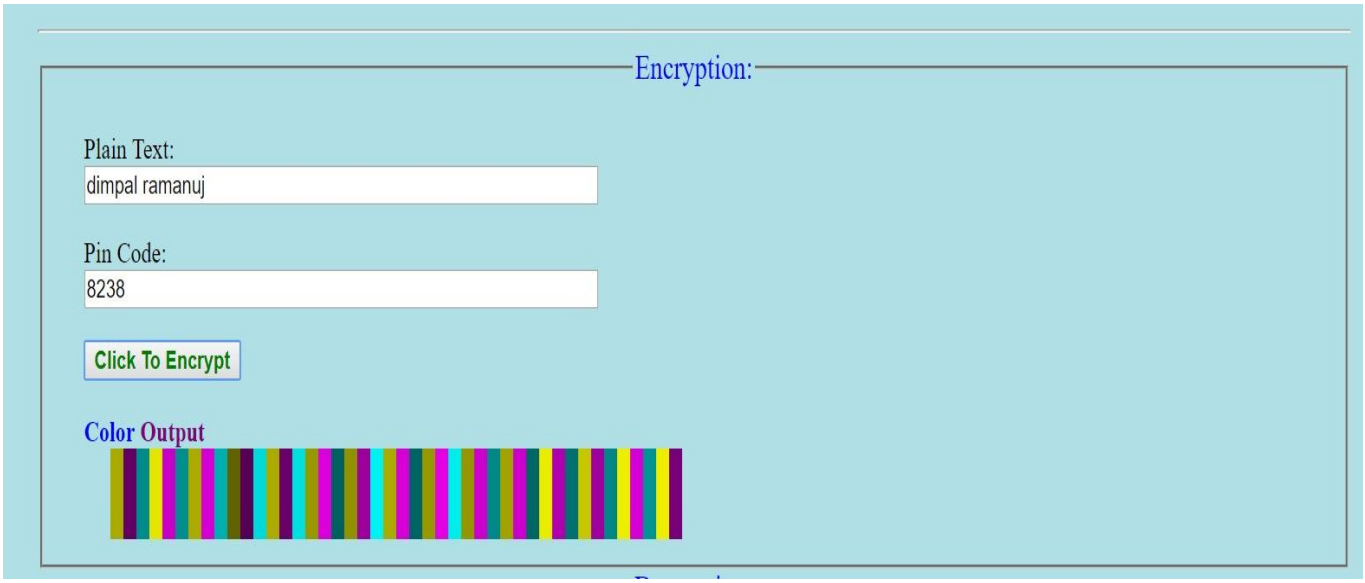
1) *Html***:** Hypertext Markup Language is the standard markup language for creating web pages and web applications. With Cascading Style Sheets and JavaScript, it forms a triad of cornerstone technologies for the World Wide Web.
2) *CSS:* Cascading Style Sheets is a style sheet language used for describing the presentation of a document written in a markup language like HTML. CSS is a cornerstone technology of the World Wide Web, alongside HTML and JavaScript
3) *Javascript:* JavaScript, often abbreviated as JS, is a high-level, interpreted programming language that conforms to the ECMAScript specification. JavaScript has curly-bracket syntax, dynamic typing, prototype-based object-orientation, and first-class functions

Flowchart for encryption and decryption



C. Screenshots

1) *Encryption:* when the webpage is loaded, we are displayed with blocks for encryption and decryption.
As we enter the Plaintext: dimpal ramanuj and Pin: 8238

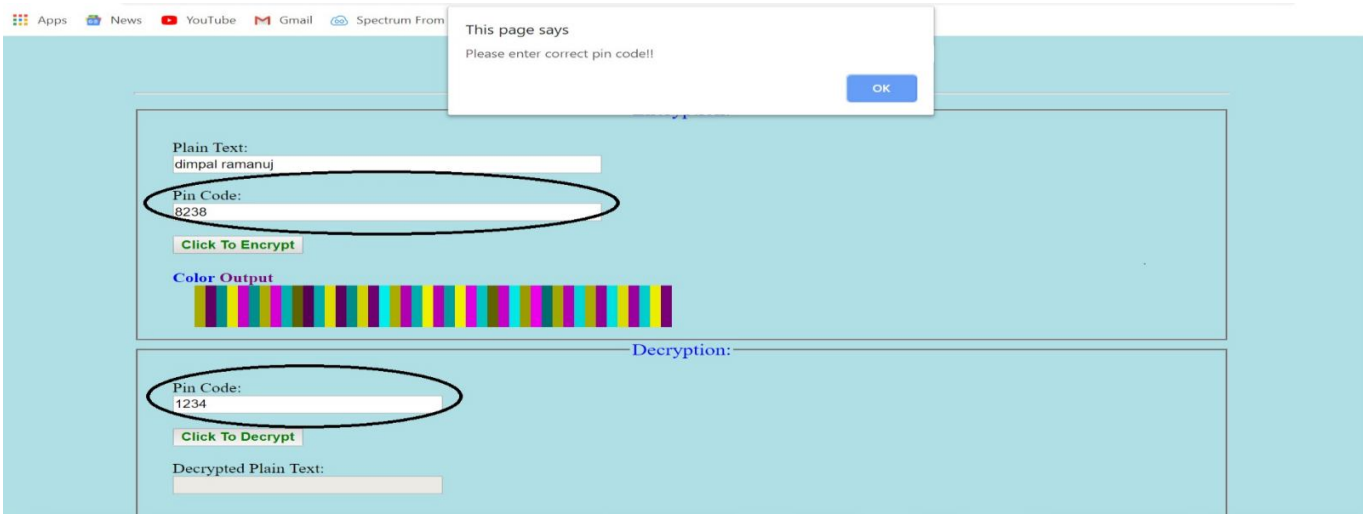


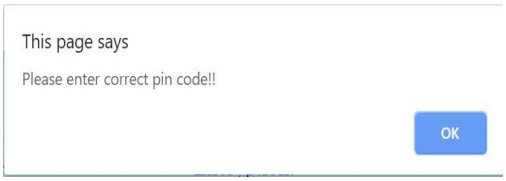
D. Output

In the above screenshots we can see the user tries to encrypt the plaintext into cipher colour block using pin code as the key. The input goes through different encryption one by one and then converted to color block output. User gets the above output which is the color block from a set of input which is text and numeric. The operations are performed on the above set of input “dimpal ramanuj” and “8238” pin number the generate the coloured output.

E. Decryption

Case 1: Wrong Pin If the pin entered does not match your encryption pin the popup box displays which shows that your pin does not match and renter correct pin.





In the above example, user wants to decrypt the color code. So according to the principle of encryption decryption, we need a key. Here pin is the key. What if the user unknowingly enters wrong pin? The popup is displayed saying you have to enter pin correct.

Case 2: Correct Pin

In the above screenshot we see that the user gets back the plain text from the cipher colour block, if the pin he entered at the time of encryption is same as that at time of decryption.

This above operation is performed as a combination of different types of encryption techniques which uses plaintext of one for others input and decryption is vice versa. Pin is used at the third stage when AES comes into picture. But during decryption it is needed at initial or start stage as the combination are also reversed.

V. RESULTS

In the above environment, we wish to show an encryption technique which uses different encryption/decryption techniques in all to get an output.

The input is given to the above environment and output is a colour block.

According to the above observation, we can see that the user is able to get a color block cipher in output which is generated from a set of input in the form of text or numerals.

Also, there is a pin code associated with the whole process which is used as a key in our scenario.

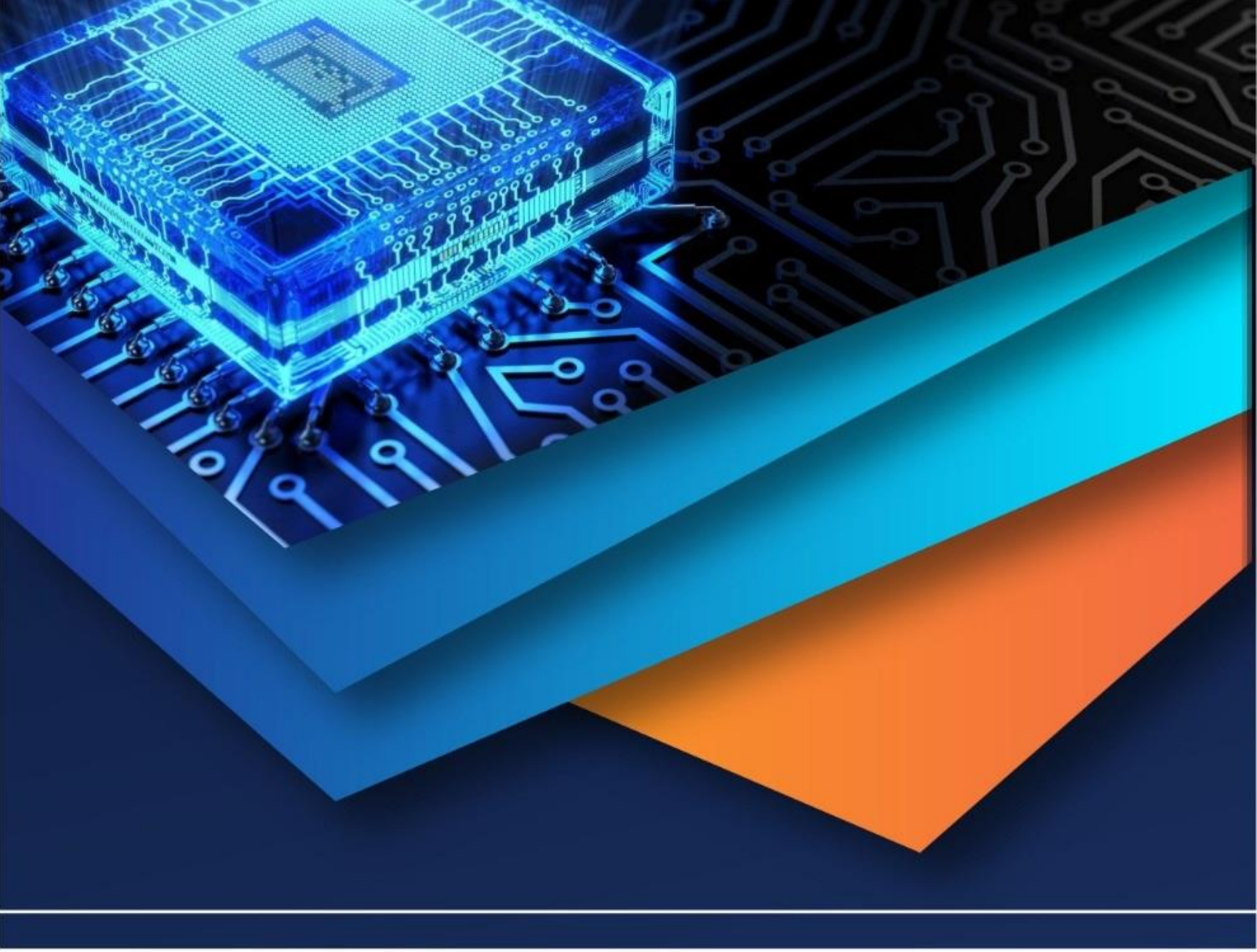
The user gives the plaintext and pin in the page we created using basic scripting and programming language and then we are able to create desired cipher coloured block of output.

VI. CONCLUSION

To compensate the need for the internet security we have to provide a complex cryptographic algorithm as proposed by this paper. In this thesis we have use a combination of different cryptographic or we say encryption techniques in one algorithm and developed an environment. Also, we have twisted the output by getting coloured cipher block instead of text and numerals.

REFERENCES

[1] https://en.wikipedia.org/wiki/Cryptography
[2] https://blog.irdeto.com/2016/08/15/cryptography-is-everywhere-in-day-to-day-life/
[3] https://www.veryshortintroductions.com/view/10.1093/actrade/9780192803153.001.0001/actrade-9780192803153
[4] D. g. Zoran Hercigonja, "Comparative Analysis of Cryptographic Algorithms," 2016.
[5] M. E. H. Whitfield Diffie, "New Directions in Cryptography," 1976.
[6] D. A. N. I. E. L. TEMKIN, "UNUSABLE FOR PROGRAMMING," 2017.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY