International Journal of
Statistics and Applied Mathematics

ISSN: 2456-1452
Maths 2024; 9(2): 43-46
© 2024 Stats & Maths
https://www.mathsjournal.com
Received: 09-01-2024
Accepted: 13-02-2024

Manoj Sharan
Department of Mathematics
BMU, Rohtak, Haryana, India

Kamal Kumar
Department of Mathematics
BMU, Rohtak, Haryana, India

Inderjit Singh
Department of mathematics,
Dayanand College Hisar,
Haryana, India

Permutation, additive and multiplicative group block cipher

Manoj Sharan, Kamal Kumar and Inderjit Singh

Abstract
In this paper, we proposed a technique to encrypt and decrypt a message using additive, multiplicative and permutation group. We focus mainly on increasing the layers of encryption and hence increasing the complexity of decryption performed by attacker. Three different layers of encryption can protect original message more efficiently.

Keywords: Cryptography, block cipher, encryption, decryption, permutation group

Introduction

Communication is fundamental to the existence and survival of humans as well as to an organization. It is a process of sharing ideas, information, views and facts from one place, person or group to another. Different ways to communicate through internet are e-mails, social networks, audio-video conferencing and chat room. Cryptography is a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it. This paper provides a technique which encodes the data in blocks and then encrypts and decrypts it. Using this technique, data can be encrypted in unreadable form. Internet may have third party interference, but the data will be secure with its confidentiality and integrity. Internet is a channel of communication between billions of people and there is a great increase in its use even for commercial purposes. Due to these, security becomes a tremendously important issue to deal with. Cryptography is the best way to secure a message. Confidentiality and integrity of message is the biggest concern for most of the network applications. If the trend of online communication continues then there will be a need to develop better cryptographic techniques. This paper presents an efficient encryption and decryption algorithm using block cipher. The message is changed using group properties and then encoded into blocks after that permutation is also used. Thus the resultant output of the encrypted text is computationally secure, usually named as cipher text. Hence, the proposed technique will be secure and provides the confidentiality and integrity of message.

In this paper, we proposed a technique to encrypt and decrypt a message using additive, multiplicative and permutation group, the encrypted message is converted into blocks and the blocks are also encrypted using permutation.

2. Block Cipher

In this cipher, a block of plain text is treated as a whole and used to produce the Ciphertext of equal length. Typically a block size of 64 and 128 bits is used. It is both symmetric and asymmetric key cipher. Key will be applied on each block. Plain Text is divided into blocks each block size is 64 bits, key is used on each block to generate cipher text in blocks each block size is 64 bits. DES, AES, RSA are block cipher.

3. Problem Definition and Novelty

This paper presents an efficient encryption and decryption technique with block cipher. The original message is encrypted with more security layers. More encrypted layers will provide enhanced security. Here the cipher text is three times encrypted original message. Instead of using only block cipher, here symmetric group is also used.

Corresponding Author:
Manoj Sharan
Department of Mathematics
BMU, Rohtak, Haryana, India

4. Proposed technique

In this proposed technique the original message is encrypted using symmetric group, the encrypted message is converted into blocks and the blocks are also encrypted using permutation. We focus mainly on increasing the layers of encryption and hence increasing the complexity of decryption performed by attacker. Three different layers of encryption can protect original message more efficiently.

5. Multiple Layers Cryptographic Algorithm

This algorithm has following steps.

5.1 Encryption

- **Layer 1:** The original message is treated as a symmetric group where the order of the group is the length of original message. Each place value of the message which has multiplicative inverse is permuted with their multiplicative inverse and the remaining are permuted with their additive inverse.
- **Layer 2:** The encrypted message provided by Layer 1 is encoded into blocks. Using ASCII each digit is treated as MessageByte[i] and encoding is done as $\text{MessageByte}[i]\times(\text{Byte\_Size})^{i\ \text{modulo(Block Size)}}$
- **Layer 3:** BlockInts given by Layer 2 are also treated as elements of a symmetric group where the order of the group is the number of BlockInts. Each BlockInt which has multiplicative inverse is permuted with their multiplicative inverse and the remaining are permuted with their additive inverse.
- The Ciphertext formed using these three layers can be transmitted through unsecured network.

5.2 Decryption

- The Ciphertext received can be decrypted layer by layer.
- **Decryption of Layer 3:** The whole Ciphertext is treated as a symmetric group where the order of the group is the number of BlockInts. Each BlockInt which has multiplicative inverse is permuted with their multiplicative inverse and the remaining are permuted with their additive inverse.
- **Decryption of Layer 2:** The decrypted text in the forms of BlockInts provided by Layer 3 is decoded. Here ASCII Number = BlockInt ÷ $(\text{Byte\_Size})^i$ and BlockInt modulo $(\text{Byte\_Size})^i$ where i = Block Size-n and n = 1, 2, 3…Block Size-1.
- **Decryption of Layer 1:** The whole decrypted text provided by Layer 2 is treated as symmetric group where order of the group is the length of decrypted text. . Each place value of the text which has multiplicative inverse is permuted with their multiplicative inverse and the remaining are permuted with their additive inverse.

6. Example

(a) Encryption

Here the original message is:

Cryptography refers to secure information and communication techniques derived from mathematical concepts and a set of rule-based calculations called algorithms, to transform messages in ways that are hard to decipher.

Step 1: Encryption by Layer 1

Crrrhaiwec rtldyad srl aht srac niostg-sfed hrafmnore to, amht r g afdnlpaa rnsimaau lpcmd scbaepuo soetrsoa dta stp cyod oavitaseotsmom r hecieem oerqonmcctcniinatiou mncideaenlicatrofrifeeueee ttsse eu nhlanghtly.

Step 2 : Encoding by Layer 2

```
[161358016901852795551151128253129978435, 132099545693962303755393212579559007329,
129529149369980876547448772229245529632, 43139720337249606779918639895141051750,
153434686929838015832385426974837252210, 129445977763087632903555754246375828841,
154710333953635207813124513488042291301, 154738039725053388947968813933471670369,
132120105481360160230312239047236744033, 132197893854302936036016846518725469545,
134773394790901735540412035308483864942, 134778526717130285069133329388847129953,
146383614089808068713646036850558985589, 219468729230969373027432]
```

Step 3 : Encryption by Layer 3

```
[161358016901852795551151128253129978435, 132099545693962303755393212579559007329,
146383614089808068713646036850558985589, 129445977763087632903555754246375828841,
134773394790901735540412035308483864942, 43139720337249606779918639895141051750,
132120105481360160230312239047236744033, 154738039725053388947968813933471670369,
154710333953635207813124513488042291301, 134778526717130285069133329388847129953,
153434686929838015832385426974837252210, 132197893854302936036016846518725469545,
129529149369980876547448772229245529632, 219468729230969373027432]
```

The outcome of Step 3 is final Cipher text which is transmitted through unsecured network.

(b) Decryption

Step 1: Decrypting the Layer 3 of the received Cipher text

```
[161358016901852795551151128253129978435, 132099545693962303755393212579559007329, 129529149369980876547448772229245529632,
43139720337249606779918639895141051750, 153434686929838015832385426974837252210, 129445977763087632903555754246375828841,
154710333953635207813124513488042291301, 154738039725053388947968813933471670369, 132120105481360160230312239047236744033,
132197893854302936036016846518725469545, 134773394790901735540412035308483864942, 134778526717130285069133329388847129953,
146383614089808068713646036850558985589, 219468729230969373027432]
```

Step 2: Decrypting the Layer 2

Crrrhaiwec rtldyad srl aht srac niostg-sfed hrafmnore to,amht r g afdnlpaa rnsimaau lpcmd scbaepuo soetrsoa dta stp cyod oavitaseotsmom r hecieem oerqonmcctcniinatiou mncideaenlicatrofrifeeueee ttsse eu nhlanghtly.

Step 3: Decrypting the Layer 3

Cryptography refers to secure information and communication techniques derived from mathematical concepts and a set of rule-based calculations called algorithms, to transform messages in ways that are hard to decipher.

Hence, the outcome of Step 3 is required decrypted text.

7. Practical Implementation

We have implemented the proposed technique of encryption and decryption algorithms by the help of a Python program. The Python program performs the encryption and decryption operations within few milliseconds.

The practical platform details are

Table 1: Platform details

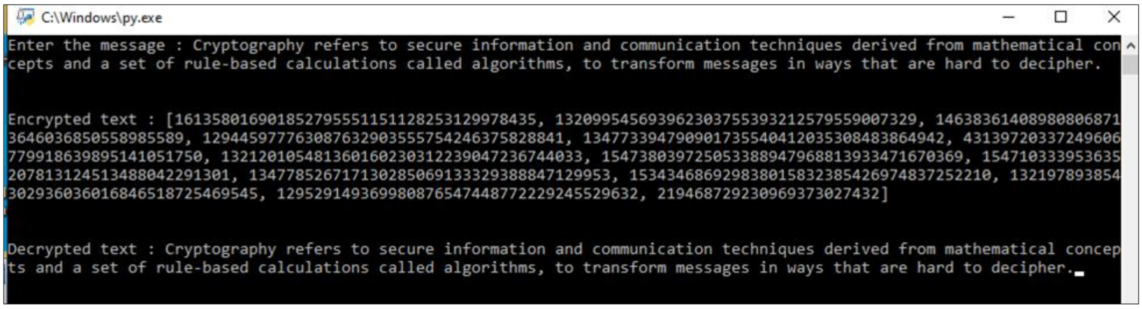
Component	Value
Processor	Intel Core i5
OS	Windows 10
Ram	4 GB

Table 1. Represents platform details on which we have tested proposed technique.

Table 2: Trailed Strings

Message	Encrypted message	Decrypted message
Cryptography refers to secure information and communication techniques derived from mathematical concepts and a set of rule-based calculations called algorithms, to transform messages in ways that are hard to decipher.	[161358016901852795551151128253129978435, 132099545693962303755393212579559007329, 146383614089808068713646036850558985589, 129445977763087632903555754246375828841, 134773394790901735540412035308483864942, 43139720337249606779918639895141051750, 132120105481360160230312239047236744033, 154738039725053388947968813933471670369, 154710333953635207813124513488042291301, 134778526717130285069133329388847129953, 153434686929838015832385426974837252210, 132197893854302936036016846518725469545, 129529149369980876547448772229245529632, 219468729230969373027432]	Cryptography refers to secure information and communication techniques derived from mathematical concepts and a set of rule-based calculations called algorithms, to transform messages in ways that are hard to decipher.
Cryptography is the study of secure communications techniques that allow only the sender and intended recipient of a message to view its contents.	[145054367022544981387021241922486497859, 151700201580097862371325329085222511461, 146819726645553624920764067459485689189, 133522154062024461829467306360342667621, 43051755533695424975424999719653241888, 134778912001831280375923931699256320800, 43098303819613558020070148281674854515, 154763717569429459120355622021128089700, 152053359922659462698760081820296897312, 11897]	Cryptography is the study of secure communications techniques that allow only the sender and intended recipient of a message to view its contents.
Cryptographic systems are used extensively, to ensure secrecy and authenticity of sensitive information. Cryptography allows us to transmit data in such a way, that it is understood only at the receiver end.	[134768405472567766160104471721177805379, 129539803418673816702382522350176333344, 154357252617095457724026604911579785504, 146830030976521944972146992461070166126, 145490194888701461211792644963960823905, 43113616164346743547394595264542023796, 152079238929425449801821266351463407731, 161378561848297557014230231697673512303, 146731396804882983772116727308977468276, 43062032609122483605151599598625911584, 154767450329201830573115615365090601317, 152157287152278226766784950893211316839, 239787556756461672638320363155513721]	Cryptographic systems are used extensively, to ensure secrecy and authenticity of sensitive information. Cryptography allows us to transmit data in such a way, that it is understood only at the receiver end.

Table 2 depicts different trailed strings.

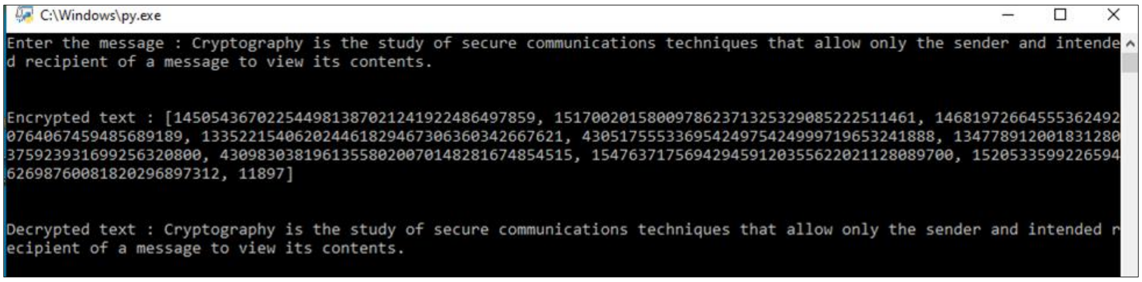


```
Enter the message : Cryptography refers to secure information and communication techniques derived from mathematical con
cepts and a set of rule-based calculations called algorithms, to transform messages in ways that are hard to decipher.


Encrypted text : [161358016901852795551151128253129978435, 132099545693962303755393212579559007329, 14638361408980806871
3646036850558985589, 129445977763087632903555754246375828841, 134773394790901735540412035308483864942, 43139720337249606
779918639895141051750, 132120105481360160230312239047236744033, 154738039725053388947968813933471670369, 154710333953635
207813124513488042291301, 134778526717130285069133329388847129953, 153434686929838015832385426974837252210, 132197893854
302936036016846518725469545, 129529149369980876547448772229245529632, 219468729230969373027432]


Decrypted text : Cryptography refers to secure information and communication techniques derived from mathematical concep
ts and a set of rule-based calculations called algorithms, to transform messages in ways that are hard to decipher._
```

Fig 1: Shows the snapshot of encryption and decryption process of the string “Cryptography refers to secure information and communication techniques derived from mathematical concepts and a set of rule-based calculations called algorithms, to transform messages in ways that are hard to decipher

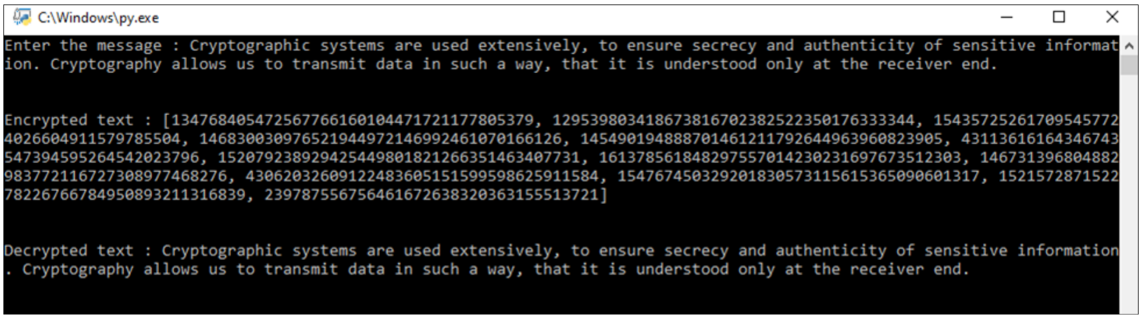


```
Enter the message : Cryptography is the study of secure communications techniques that allow only the sender and intende
d recipient of a message to view its contents.


Encrypted text : [145054367022544981387021241922486497859, 151700201580097862371325329085222511461, 14681972664555362492
0764067459485689189, 133522154062024461829467306360342667621, 43051755533695424975424999719653241888, 134778912001831280
375923931699256320800, 43098303819613558020070148281674854515, 154763717569429459120355622021128089700, 1520533599226594
62698760081820296897312, 11897]


Decrypted text : Cryptography is the study of secure communications techniques that allow only the sender and intended r
ecipient of a message to view its contents.
```

Fig 2: Shows the snapshot of encryption and decryption process of the string “Cryptography is the study of secure communications techniques that allow only the sender and intended recipient of a message to view its contents



```
Enter the message : Cryptographic systems are used extensively, to ensure secrecy and authenticity of sensitive informat
ion. Cryptography allows us to transmit data in such a way, that it is understood only at the receiver end.


Encrypted text : [134768405472567766160104471721177805379, 129539803418673816702382522350176333344, 15435725261709545772
4026604911579785504, 146830030976521944972146992461070166126, 145490194888701461211792644963960823905, 43113616164346743
547394595264542023796, 152079238929425449801821266351463407731, 161378561848297557014230231697673512303, 146731396804882
983772116727308977468276, 43062032609122483605151599598625911584, 154767450329201830573115615365090601317, 1521572871522
78226766784950893211316839, 239787556756461672638320363155513721]


Decrypted text : Cryptographic systems are used extensively, to ensure secrecy and authenticity of sensitive information
. Cryptography allows us to transmit data in such a way, that it is understood only at the receiver end.
```

Fig 3: Shows the snapshot of encryption and decryption process of the string” Cryptographic systems are used extensively, to ensure secrecy and authenticity of sensitive information. Cryptography allows us to transmit data in such a way, that it is understood only at the receiver end.

8. Conclusion

- The proposed techniques will not have effect of Brute Force and other Cryptanalytic attacks as three Layers of security are generated for every message that is transferred.
- To break these three Layers cannot be an easy task for external adversaries even they are using supercomputers.
- As the cipher text that is produced is computationally secure, since the cipher text generated is completely independent of the message.
- The algorithm proposed will take less time also.
- This also can be used for most crucial applications where it requires a significant security of transmitted message.

9. References

1. Hill LS. Cryptography in an algebraic alphabet. The American Mathematical Monthly. 1929;36(6):306-312.
2. Katz J, Menezes AJ, Van Oorschot PC, Vanstone SA. Handbook of Applied Cryptography. CRC Press; c1996.
3. Lidl R, Niederreiter H. Finite Fields, volume 20. Cambridge University Press; c1997.
4. Dooley JF. A Brief History of Cryptology and Cryptographic Algorithms. New York: Springer; 2013.
5. Hellman WDAM. New directions in cryptography. IEEE Transactions on Information Theory. 1976;IT-22(6):644-654.
6. Stallings W. Cryptography and Network Security Principles and Practices. New York: Prentice Hall; 2005.
7. Sharma RK, Shah SK, Sanker AG. Algebra I. Pearson, India; c2012.
8. Singh M, Kumar A, Singh K. Encryption by using matrix-added, or matrix multiplied input images placed in the input plane of a double random phase encoding geometry. Optics & Laser Engineering. 2009;47:1293–1300.
9. Singh N, Sinha A. Gyrator transform-based optical image encryption, using chaos. Optics & Laser Engineering. 2009;47:539–546.
10. Stallings W. Cryptography and Network Security. Prentice Hall, New Jersey; c2006.
11. Sui L, Gao B. Single-channel color image encryption based on iterative fractional Fourier transform and chaos. Optics and Laser Technology. 2013;48:117–127.
12. Mishra DC, Sharma RK. Grayscale-image encryption using Random Hill Cipher over SLn (Fq) associated with Discrete Wavelet Transformation. Applied and Computational Mathematics. 2013;08:777–791.
13. Kumar M, Mishra DC, Sharma RK. A first approach on an RGB image encryption. Optics & Lasers in Engineering. 2014;52:27–34.