International Journal of Engineering Trends and Technology
ISSN: 2231–5381 / https://doi.org/10.14445/22315381/IJETT-V71I8P237

Volume 71 Issue 8, 428-438, August 2023
© 2023 Seventh Sense Research Group®

Original Article

Implementation of Multi-Pass Method using Advanced Number Series Cipher Techniques in a Network Channel

V. Joseph Emmanuvel[1], E. J. Thomson Fredik[2]

[1]*Department of Computer Science, Karpagam Academy of Higher Education, Coimbatore, Tamilnadu, India.*
[2]*Department of Computer Technology, Karpagam Academy of Higher Education, Coimbatore, Tamilnadu, India.*

[1]*Corresponding Author: josejan1978@gmail.com*

Received: 25 January 2023 Revised: 30 June 2023 Accepted: 05 August 2023 Published: 15 August 2023

Abstract *- As far as the need for computers has become more for almost all communication functions, the essentiality of automated tools for safeguarding files and messages and, of course, other significant information available n the individual's computer has to be highly secured. To get the messages transmitted to be secured, the information has to be protected or hidden or changed in a diverse design where only the two authorized communicating individuals can know what actually is happening in the communication channel. Confidentiality, integrity and availability of the message have to be perfectly authorized. Computer Security is the widespread name we use for compiling considered tools to protect data from nosy people, attackers and hackers. Nowadays, since millions and millions of people have started using computer networks for various operations like banking, income tax filing returns, buying and selling, online purchase, ordering of goods, etc., the need for security is being threatened from the perspective of a potentially immense problem. In this attachment, an innovative method should be designed to carry out, making sure the security of data transmission between two persons. That, too, this newly proposed procedure should be designed such that no challenger can prevail over its principle. The main motive of the secret message is to generate security in the algorithm. While starting to concentrate on designing the new security model, that particular model has to be created for the distribution cum allotment of covert data. In this research paper, a new method is recommended where. The implementation of the multi-pass protocol method using an advanced number series cipher technique is utilized to encrypt and decrypt a message in a network channel using Symmetric Key Encryption.*

Keywords *- Mathematical series cipher, Multi pass protocol, Decryption, Cryptography, Encryption.*

1. Introduction

During the past period, computer network system was, for the most part, utilized only by the research scholars of colleges and universities for making communiqué using mail. Also, some commercial employees use the same for sharing devices like printers. Hence the need for security was not given a large amount of significance at that time. Everything has changed upside down nowadays. It is a well-known fact that most people have started utilizing computers and networks for online shopping, transferring amounts through online banking, uploading online applications, filing tax returns, payment for electricity bills, applying for online certificates, etc. Hence the need for security plays a pivot role now while these things are done. Security is concerned with avoiding inquisitive people who try to read others' messages or modify the same by illegally entering others' communication channels. It is concerned with persons who try to access remote services that they, in point of fact, are not allowed to use. Almost plenty of security-related issues have been deliberately caused by malicious human beings who incessantly attempt to earn benefits or trouble somebody. Some common activities and disturbances of the malicious people who create security issues, like troubling the communication processes or intervening in a private communication channel, have been listed below in Table – 1.

Table 1. Security issues created by various users

User	Intention
Terrorist	Stealing army secrets
Secret Agent	Knowing the opponent's strength
Accountant	Stealing money from an organization
Businessman	Knowing other company's project
Hacker	Stealing other's information
Student	Knowing other's messages or mail
Banker	Steal debit or credit card numbers.

This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/)

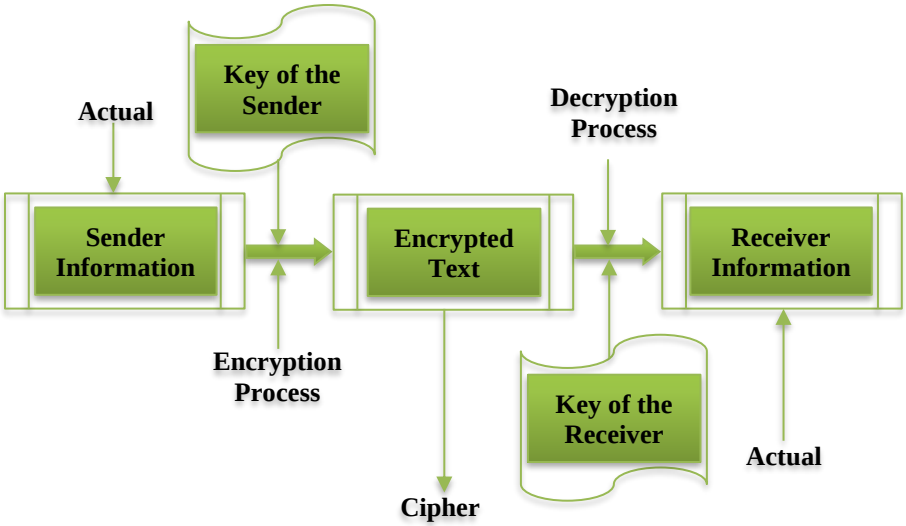

Fig.1 Process of cryptography

Because the potential of computer storage is much elevated, information security is more frequently needed to safeguard data while it is sent in a network. Malevolent human beings make use of this choice to get in the way and capture the message other than the actual communicating individuals. Such nosy people cannot be prevented from their interfering with actions like meddling in others' communication. The no more alternative to providing security to our data is to progress it in a dissimilar arrangement, and the individuals who are actually alive in the communication process alone can understand the unique data. In [1], William Stallings, 2006 described the technique to decipher information possessing, having no knowledge about, the enciphering feature called cryptography. He mentioned that a strong encrypting algorithm is needed such that those who have an idea about the algorithm cannot get the original text or secret key at any cost. In the facet to prevail over such issues in the current system, a novel, innovative method has been proposed where multi-pass protocol schemes have been taken into consideration, which uses advanced series concepts to convert the original message, which travels in a dedicated network utilizing several, unlike keys in every pass. The conventional procedure of cryptography is depicted in Fig 1.

2. Survey of Literature

Commonly there are two broad categories of processes involved in the traditional cryptographic process.

- Symmetric Key process
- Asymmetric Key process.

2.1. Symmetric Key Encryption Process

In [2], Behrouz A Forouzan and Debdeep Mukhopadhyay, 2015 precisely quoted that the Symmetric Key Encryption process is also called Secret Key Encryption or Secret Key Cryptography. In this process, a person sends information to another person in a communication channel such that an intruder who wants to know the fact of the actual message traveling in the channel will be unable to know the same. The sender and receiver automatically encrypt and decrypt the message with their individual keys. The Symmetric Key algorithms used for Conventional Encrypting are clearly depicted below in Table - 2.

Table 2. Symmetric key algorithm for conventional encrypting

ID Based Encryption	Description
0	Nil Encryption
1	IDEA (International Data Encryption Algorithm)
2	Triple DES (Data Encryption Standard)
3	CAST – 128
4	Blowfish
5	SAFER (Secure and Fast Encryption Routine) – SK Symmetric Key – 128
6	Reserved for DES / SK
7	Reserved for AES–128
8	Reserved for AES–192
9	Reserved for AES–256
100 – 110	Private Algorithm

In [3], Joseph Emmanuvel. V et al., 2020 pointed out an approach of implementing a process in a channel using number cipher series as the pivot key for encryption and decryption using three variable keys at every first, second and third pass. In [4], Fuyuki Kitagawa, Ryo Nishimaki & Keisuke Tanaka, 2022 gave a secret key encryption algorithm where the keys 8, 25, 27, 34, 53, 65, 70, and 74 were used for functional encryption till then it is only a single pass process.

In [5], Boni Oktavianab&Andysah Putera Utama Siahaan, 2016 suggested a new cryptographic technique which makes use of the implementation of a protocol with three passes where the Caesar Cipher technique has been implemented and the numeral number 3 was the key used with various shift values. Such methods used similar keys for all passes.

In [6], Priya Thakur & Anurag Rana, 2016 proposed that the most vital objective of using a symmetric key encipherment technique is that a single secret key has been made into used for encrypting and decrypting. Asymmetric Key Encipherment, referred to as Public Key Encipherment or otherwise known as Public Key Cryptography, has a little few exceptions when compared to the former Symmetric Encryption. Actually, there are two keys for encryption and decryption. The sender on the sender's side uses a public key for encryption where, and the receiver on the destination side uses a private key for decryption.

In [7], Ayush, 2010 described that the Secure Socket Layer, Diffie – Hellmen Key Exchange, Rivest–Shamir–Adleman Public key Cryptographic procedure and Secure Shell procedures were used in similar forms of symmetric processes.

In [8], Andizhan Putera, 2016 introduced a new method view where the square matrix is the key using a three-pass implementation in Hill Cipher Encryption.

In [9], Amin Subandi et al., 2017 proposed a new technique in Vigenere Cipher Cryptography in which researchers introduced a higher matrix representation as the key when compared to the previous one. In [7], Duc Manh Nguyen *et al.*, 2019 introduced a similar pass for more bits transfer making the use of likely keys in each pass.

In [10], Robbi Rahiml, 2016 described one method that a protocol, especially three passes, which allows the sender to send a converted message to a recipient by not sharing keys with the acceptor, where both never interchange keys and communication is performed in three various directions, but the keys are same.

In [11], Joseph Emmanuvel. V and Thomson Fredrik. E.J 2022 suggested a scheme with four pass protocol using numerical series for encrypting as well as decrypting, where they utilized four different keys during all four phases of changing the original text at the encrypting stage and getting back the actual text at the decrypting stage.

3. The Proposed Work

In the research work, what has been proposed is that a protocol scheme with multi-pass has been recommended, which brings into play five various passes for encryption and decryption where the advanced mathematical number series methods like triangular number series, pentagonal number series, hexagonal number series, mixed operator number series and alternate number series for every pass to convert the message.

3.1. Triangular Number Series

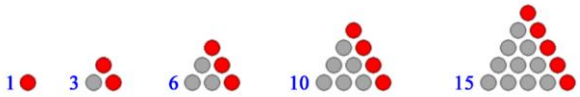

Fig. 2 Pass – I: 1, 3, 6,10, 15, 21…. Key 1 (KY1)

3.2. Pentagonal Number Series

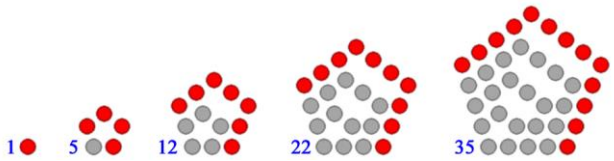

Fig. 3 Pass – II: 1, 5, 12, 22, 35,..Key 2(KY2)

3.3. Hexagonal Number Series

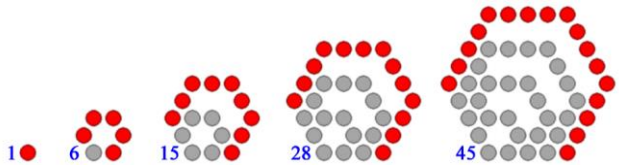

Fig. 4 Pass – III : 1, 6, 15,28, 45……Key 3(KY3)

3.4. Mixed Operator Number Series

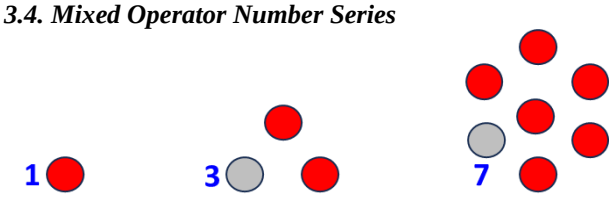

Fig. 5 Pass – IV: 1, 3, 7, 15, 31, 63, ...Key 4 (KY4)

3.5. Alternate Number Series

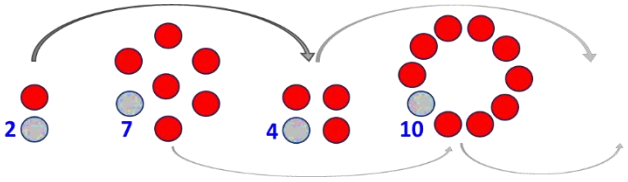

Fig. 6 Pass – V: 2, 7, 4, 10, 6, 13, ….. Key 5 (KY5)

The Encryption algorithms for each pass is

Encrypted Text1 = (AT1 + KY1) Modulo 26 ----→ First Pass (Equation - 1)

Where Encrypted Text1 = First Text Encrypted
AT1 = First Actual Text
KY1 = Key1 and
26 (English alphabet in Numbers)

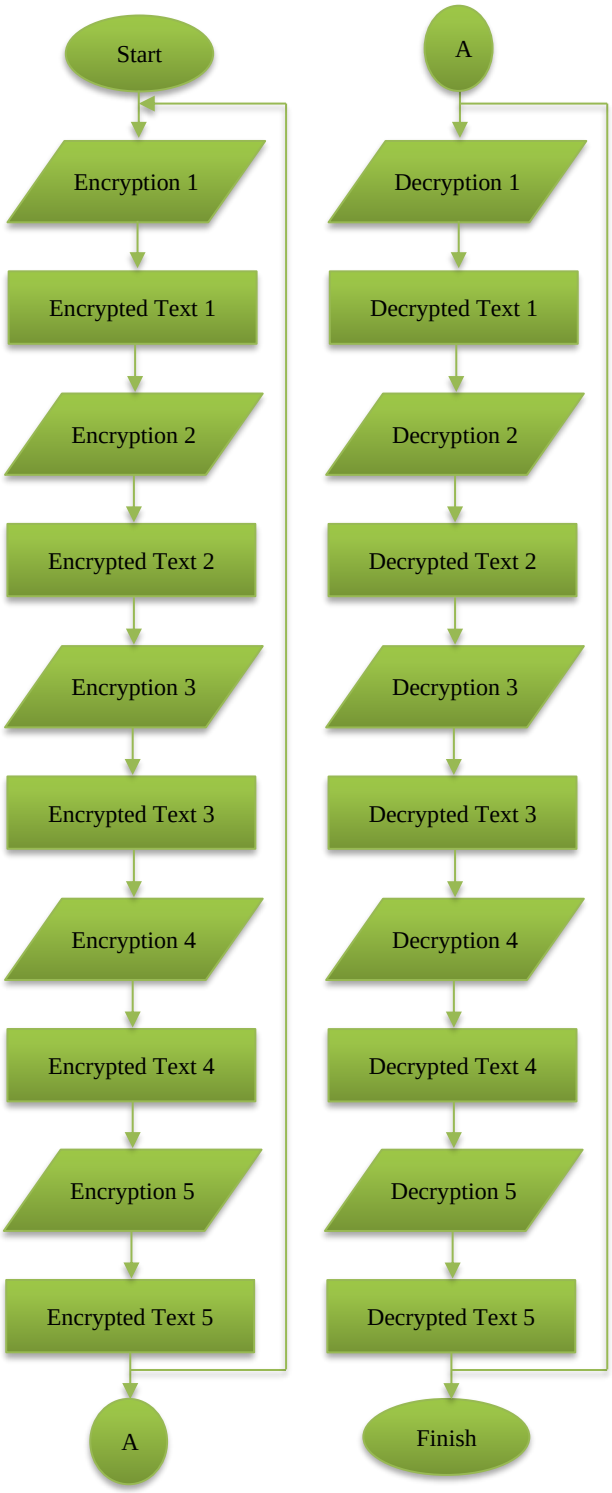

Fig. 5 Multi pass protocol scheme

Similarly,

Encrypted Text2 = (AT2 + KY2) Modulo 26 ----→ Second Pass (Equation - 2)

Encrypted Text3 = (AT3 + KY3) Modulo 26 ----→ Third Pass (Equation - 3)

Encrypted Text4 = (AT4 + KY4) Modulo 26 ----→ Fourth Pass (Equation - 4)

Encrypted Text5 = (AT5 + KY5) Modulo 26 ----→ Fifth Pass (Equation - 5)

The flow chart above below explains the multi-pass scheme.

4. Implementation and Testing

In this section, protocol scheme implementation using multi-pass and advanced mathematical series has been tested and verified. Now, let us execute our proposed algorithm by using the following original text.

4.1. Actual Text: $Cloud

As a part of improving the proposed work, the character has been included in the actual text for encryption and decryption in order to confuse intruders and malicious people. The foremost key taken by Pass one is a triangular number series. Consequently, pentagonal, hexagonal, mixed operator and alternative numbers series are considered. The encipherment takes place five times using the following procedure.

Step 1: In the first pass, the first key used is a triangular number series, and so the first triangular number 1 is used as a key in pass one.

Encrypted Text1 = (AT1 + KY1) Modulo 26 -------→ First Pass
Original text = $ (First Letter (Character))
Encrypted Text1 = ($ +1) Modulo 26
Encrypted Text1 = 1
Hence, Encrypted Text1 = %

Step 2: In the first pass, the second key used is the next subsequent number of triangular series, so number 3 is used as the key in pass one.

Encrypted Text1 = (AT1 + KY1) Modulo 26 -------→ First Pass
Original text = C (Second Letter)
Encrypted Text1 = (C + 3) Modulo 26
Encrypted Text1 = 3
Hence, Encrypted Text1 = G

Step 3: In the first pass, the third key used is the triangular number 6, which is used as the key in pass one.

Encrypted Text1 = (AT1 + KY1) Modulo 26 -----→ First Pass
Original text = L (Third Letter)
Encrypted Text1 = (L + 6) Modulo 26
Encrypted Text1 = 6
Hence, Encrypted Text1 = R

Step 4: In the first pass, the fourth key is number 10.

Encrypted Text1 = (AT1 + KY1) Modulo 26 -------→ First Pass
Original text = O (Fourth Letter)
Encrypted Text1 = (O + 10) Modulo 26
Encrypted Text1 = 10
Hence, Text1 = Y

Step 5: Similarly, the fifth key in pass one is 15.
Encrypted Text1 = (AT1 + KY1) Modulo 26 -----→ First Pass
Original text = U (Fifth Letter)
Encrypted Text1 = (U + 15) Modulo 26
Encrypted Text1 = 15
Hence, Encrypted Text1 = J

Step 6: In the first pass, the final sixth key is the numeral number 21.
Encrypted Text1 = (AT1 + KY1) Modulo 26 ------- Pass – I
Original text = D (Sixth Letter)
Encrypted Text1 = (D + 21) Modulo 26
Encrypted Text1 = 21
Hence, Encrypted Text1 = Y

The ultimate changed text obtained in pass one is portrayed in Table – 3.

Table 3. Text encrypted in first pass

PROCESS OF ENCRYPTION I						
AT	**$**	**C**	**L**	**O**	**U**	**D**
ET	**%**	**G**	**R**	**Y**	**J**	**Y**

In Table – 3, the encrypted text gained is %GRYJY. Similarly, the second key in the second pass is a pentagonal number series. This process continues as we did in the first pass but with a different key.

Table 4. Text encrypted in second pass

PROCESS OF ENCRYPTION II						
AT	**%**	**G**	**R**	**Y**	**J**	**Y**
ET	**&**	**L**	**D**	**U**	**S**	**X**

In Table –4, the encrypted text got is &LDUSX. The third key used in the third pass is a hexagonal number series.

Table 5. Text encrypted in third pass

PROCESS OF ENCRYPTION III						
AT	**&**	**L**	**D**	**U**	**S**	**X**
ET	**‘**	**R**	**S**	**W**	**L**	**L**

In Table – 5, the encrypted text encountered is ’RSWLL. In the fourth pass, Table – 6 gives the Encrypted text using a mixed operator number series.

The fourth key used in the fourth pass is a mixed operator number series.

Table 6. Text encrypted in fourth pass

PROCESS OF ENCRYPTION IV						
AT	**‘**	**R**	**S**	**W**	**L**	**L**
ET	**(**	**U**	**Z**	**L**	**Q**	**W**

In Table - 6, the mixed operator number series has been applied to alter the actual text to enciphered text in the fourth pass.

Encrypted data in the fourth pass is (UZLQW. In a similar way, in Table - 7, the alternate number series has been implemented to alter the original text to encrypted text in the final (fifth) pass.

Table 7. Text encrypted in fifth pass

PROCESS OF ENCRYPTION V						
AT	**(**	**U**	**Z**	**L**	**Q**	**W**
ET	**)**	**W**	**G**	**P**	**A**	**C**

The encrypted text in the eventual (Fifth) pass is)WGPAC.

On the other hand, the receiver decrypts the enciphered text in the antithesis order five times. Here, alternate, mixed operator, hexagonal, pentagonal and triangular numbers series are used for conversion activities on all five passes in the antithesis order for obtaining back actual text. The process is given below.

Table 8. Text decrypted in fifth pass

PROCESS OF DECRYPTION V						
ET	**)**	**W**	**G**	**P**	**A**	**C**
DT	**(**	**U**	**Z**	**L**	**Q**	**W**

Since we have to implement the other four passes, the decrypted text is still incomprehensible. The decryption process continues for the remaining four passes.

Table 9. Text decrypted in fourth pass

PROCESS OF DECRYPTION IV						
ET	**(**	**U**	**Z**	**L**	**Q**	**W**
DT	**‘**	**R**	**S**	**W**	**L**	**L**

Table 10. Text decrypted in third pass

PROCESS OF DECRYPTION III						
ET	**‘**	**R**	**S**	**W**	**L**	**L**
DT	**&**	**L**	**D**	**U**	**S**	**X**

Table 11. Text decrypted in second pass

PROCESS OF DECRYPTION II						
ET	**&**	**L**	**D**	**U**	**S**	**X**
DT	**%**	**G**	**R**	**Y**	**J**	**Y**

Table 12. Text decrypted in first pass

PROCESS OF DECRYPTION I						
ET	**%**	**G**	**R**	**Y**	**J**	**Y**
DT	**$**	**C**	**L**	**O**	**U**	**D**

Table 13. Three-Pass protocol process

File Size in Kilo Bytes	Encryption Duration in Milliseconds	Decryption Duration in Milliseconds
1	12.07	11.18
2	22.63	11.22
3	17.2	21.80
4	18.5	11.3
5	12.8	12.6
10	24.6	44.0
20	37.7	41.7
50	85.7	67.8
100	168.1	123.38
200	324.9	260.2
500	818.0	621.6
1000	1735.07	1251.7
2000	3893.6	2932.7

The ultimate concluding authentic text attained after the passes is $CLOUD. After a strong analysis of the proposed scheme, it has been determined and concluded that the time consumed for the new technique introduced is a little bit more than the existing three and four-pass protocol processes. But security plays a major role here instead of time comparison. The comparison statement has been displayed in Tables 13, 14& 15, respectively.

The repetition processes in all the schemes have been given in the below charts in Figures 3, 4 and 5.

Table 14. Four pass protocol process

File Size in Kilo Bytes	Encryption Duration in Milliseconds	Decryption Duration in Milliseconds
1	12.09	12.18
2	24.62	13.24
3	19.4	23.8
4	21.6	14.6
5	13.8	14.6
10	27.6	47.1
20	39.0	43.4
50	86.1	68.5
100	170.3	126.33
200	326.8	263.9
500	821.2	623.2
1000	1738.04	1253.6
2000	3896.1	2934.8

Table 15. Multi-Pass protocol process

File Size in Kilo Bytes	Encryption Duration in Milliseconds	Decryption Duration in Milliseconds
1	13.10	13.19
2	24.61	15.21
3	21.5	24.1
4	23.4	17.3
5	16.7	17.1
10	29.1	48.2
20	42.04	44.41
50	88.8	68.9
100	173.4	129.34
200	329.3	267.5
500	824.4	625.5
1000	1739.07	1255.61
2000	3899.01	2935.81

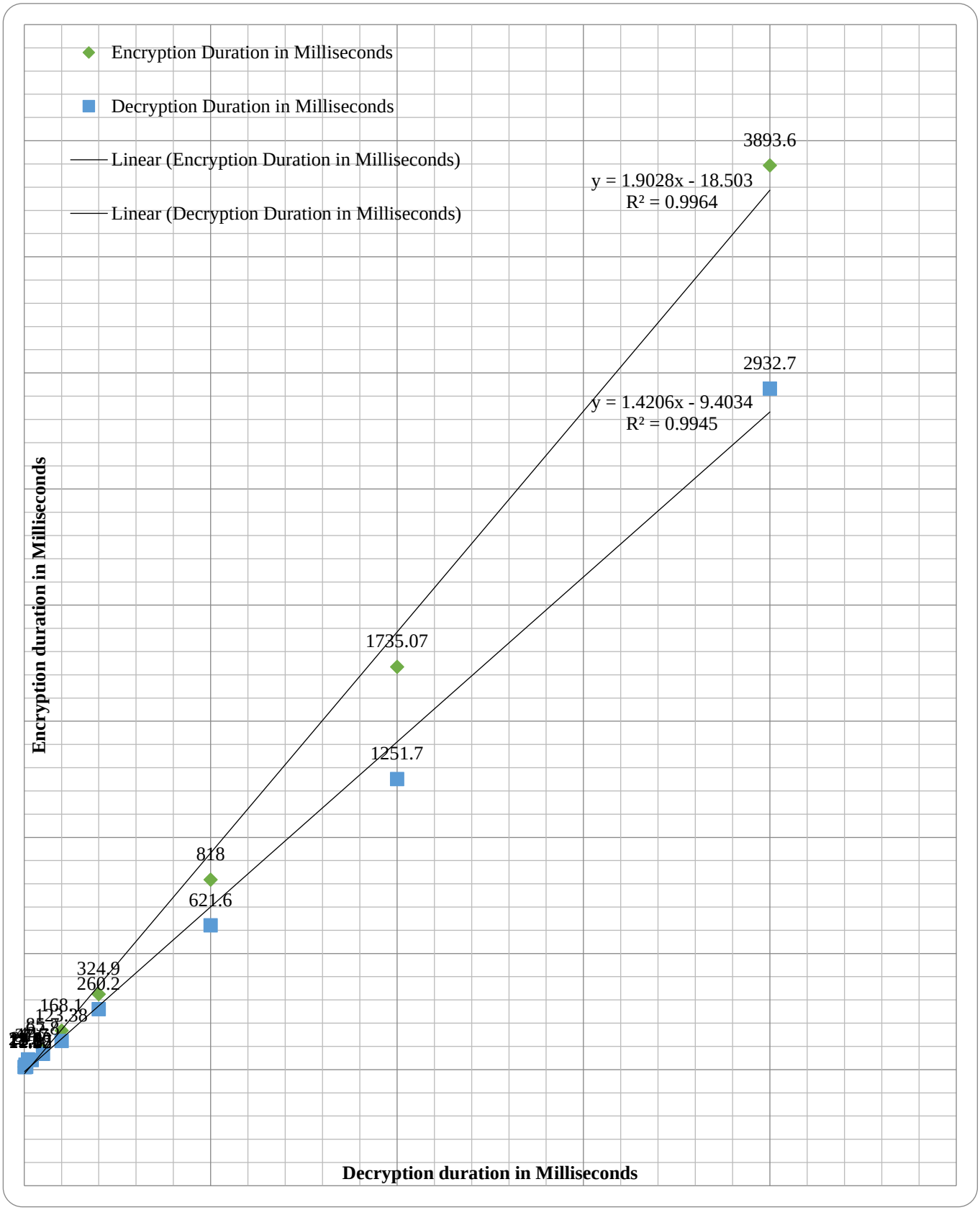

Fig. 6 Three pass scheme

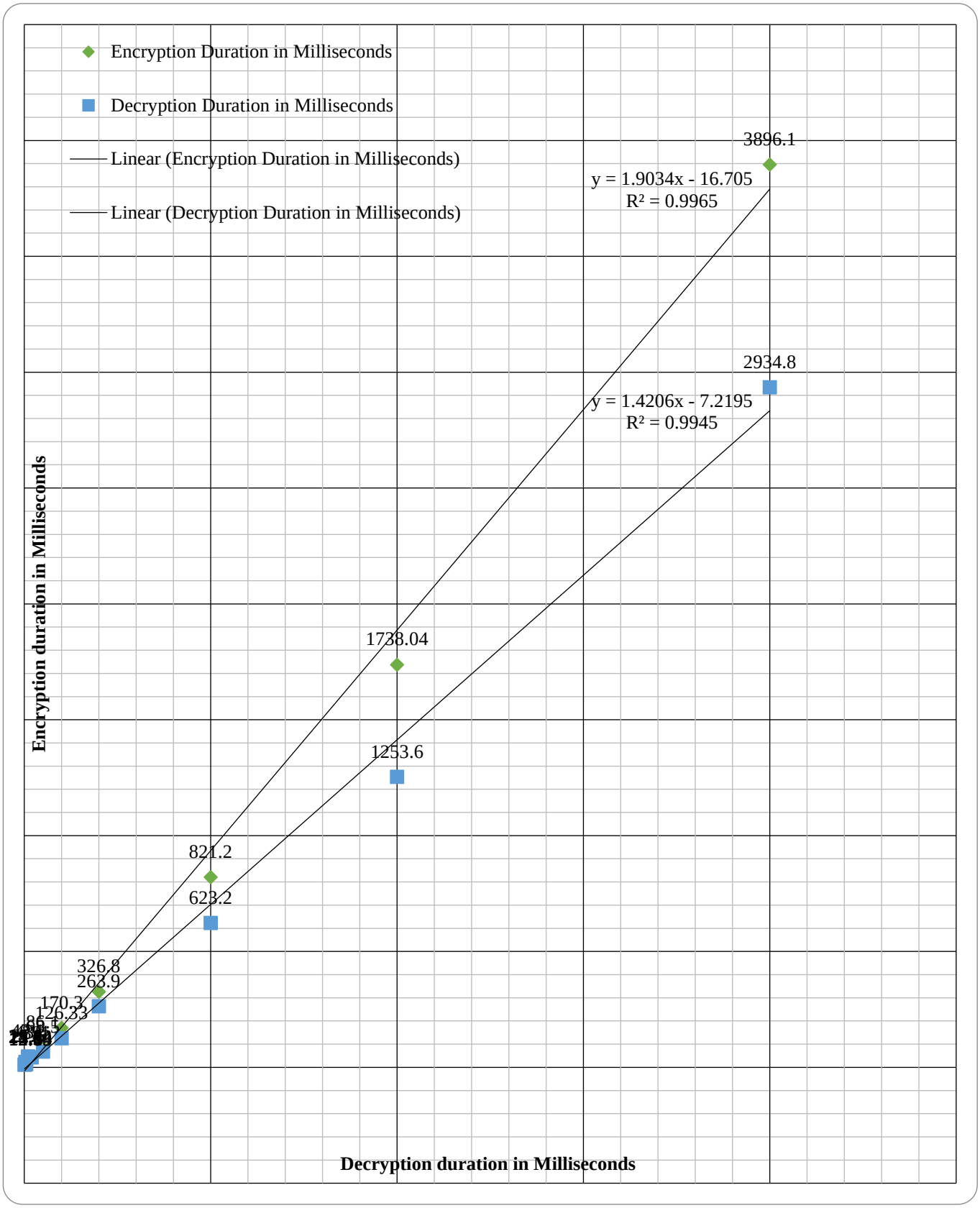

Fig. 7 Four pass scheme

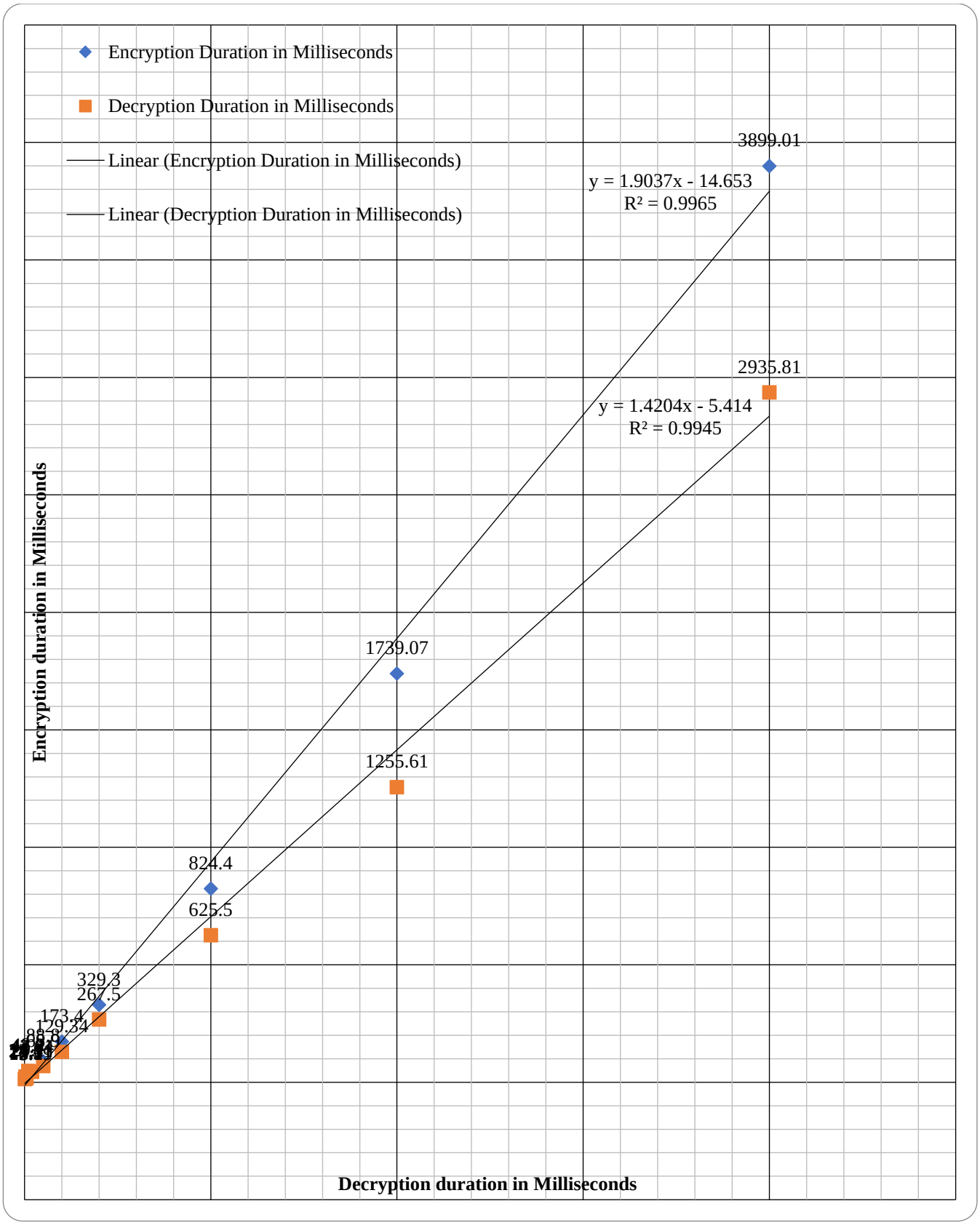

Fig. 8 Multi pass scheme

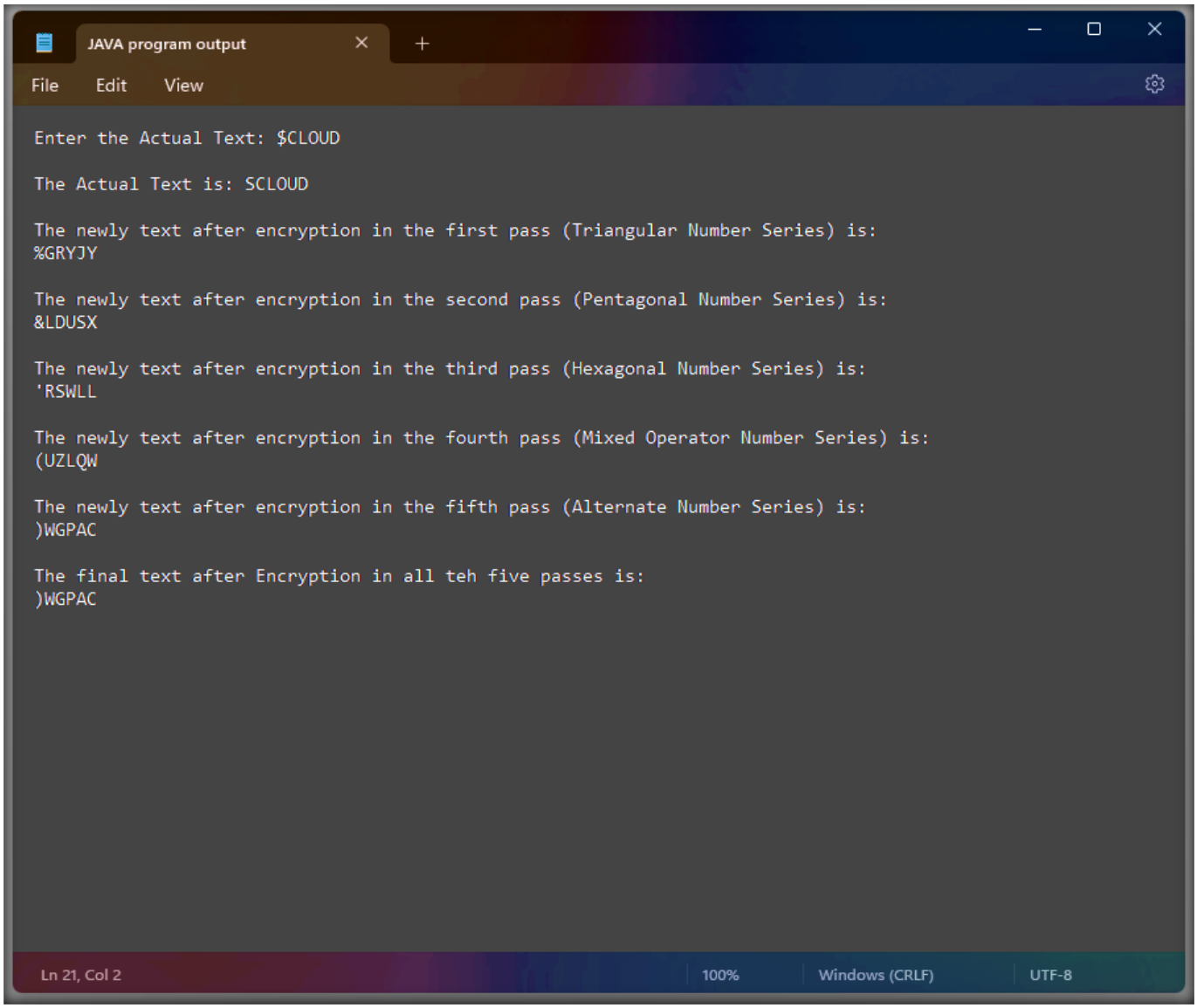

Fig. 9 JAVA program output

It has been analyzed that although the newly recommended protocol scheme with multi pass approach consumes more time than the previously available three and four pass schemes, the procedure is much better regarding the security and safety of the message in the communication channel.

This concept has been implemented in a JAVA program using string handling functions, compiled successfully, and executed. The sample output has been given below. All five passes, the triangular number series, the pentagonal triangular number series, the hexagonal triangular number series, the mixed operator triangular number series and the alternative numbers series, are used for the encryption process. The model output of the JAVA program is depicted in Figure 9.

5. Conclusion

The security and safety of the message communicated between two dedicated network channels play a significant role in cryptography. As far as protection is concerned, the data transmitted in a network should be ensured that it is fully secured in the traveling process. The newly recommended cipher scheme with the implementation of a multi-pass procedure using advanced mathematical series encipherment ensures the message passed on over a network channel is secured, and it will be impossible for the interloper to detain the authentic information. The proposed method used in five different practices assures the safety of data. As far as this research work is concerned, it is precisely found that using different keys in each pass assures much more safety while judging against all other previously accessible methods.

References

[1] William Stallings, *Cryptography and Network Security – Principles and Practices*, Third Edition, Pearson Education, Prantice Hall, 2007.

[2] Behrouz A Forouzan, and Debdeep Mukhopadhyay, *Cryptography and Network Security*, Third Edition, The McGraw Hill Companies, Inc, 2015. [Google Scholar] [Publisher Link]

[3] V Joseph Emmanuvel, and E.J Thomson Fredrik, "Three Pass Protocol Implementation using Number Cipher Encryption in a Communication Network," *Journal of Xi'an University of Architecture & Technology*, vol. 11, no. 8, pp. 1338-1341, 2020. [Google Scholar] [Publisher Link]

[4] Fuyuki Kitagawa, Ryo Nishimaki, and Keisuke Tanaka, "Obfustopia Built on Secret – Key Functional Encryption," *Journal of Cryptology*, vol. 35, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[5] Boni Oktavianab, and Andysah Putera Utama Siahaan, "Three-Pass Protocol Implementation in Caesar Cipher Classic Cryptography," *IOSR Journal of Computer Engineering*, vol. 18, no. 4, pp. 26-29, 2016. [Google Scholar] [Publisher Link]

[6] Priya Thakur, and Anurag Rana, "A Symmetrical key Cryptography Analysis using Blowfish Algorithm," *International Journal of Engineering Research & Technology*, vol. 5, no. 7, pp. 235-238, 2016. [Google Scholar] [Publisher Link]

[7] Ayushi, "A Symmetric Key Cryptographic Algorithm," *International Journal of Computer Applications*, vol. 1, no. 15, 2010. [Publisher Link]

[8] Andizhan Putera Utama Siahaan, "Three-Pass Protocol Concept in Hill Cipher Encryption Technique," *International Journal of Science and Research*, vol. 5, no. 7, pp. C-31-C-35, 2016. [CrossRef] [Google Scholar] [Publisher Link]

[9] Amin Subandi et al., "Three-Pass Protocol Implementation in Vigenere Cipher Classic Cryptography Algorithm with Keystream Generator Modification," *Advances in Science, Technology and Engineering Systems Journal*, vol. 2, No. 5, pp. 1-5, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[10] Robbi Rahim, and Ali Ikhwan, "Study of Three Pass Protocol on Data Security," *International Journal of Science and Research*, vol. 5, no. 11, pp. 102-104, 2016. [CrossRef] [Google Scholar] [Publisher Link]

[11] V. Joseph Emmanuvel, and E.J. Thomson Fredrik, "Implementation of Four-Pass Protocol Scheme using Mathematical Series Cipher Encryption and Decryption in a Communication Network," *Proceedings of International Conference on Communication and Artificial Intelligence*, vol. 435, pp. 85-96, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[12] AditiSoral, "Achieving Fully Homomorphic Encryption in Security - A Survey," *SSRG International Journal of Computer Science and Engineering*, vol. 3, no. 2, pp. 22-27, 2016. [CrossRef] [Google Scholar] [Publisher Link]

[13] Duc Manh Nguyen, and Sunghwan Kim, "A Quantum Three Pass Protocol with Phase Estimation for Many Bits Transfer," *International Conference on Advanced Technologies for Communications, IEEE*, pp. 129-132, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[14] Dian Rachmawati, and Mohammad Andri Budiman, "An Implementation of H–rabin Algorithm in the Shamir Three Pass Protocol," *International Conference on Automation, Cognitive Science, Optics, Micro – Electro Mechanical System and Information Technology (ICACOMIT), IEEE*, pp. 28-33, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[15] C. Okah, D. Matthias, and N. Nwiabu, "A Real-Time Encryption Algorithm for User Data Preservation in Mobile Computing," *SSRG International Journal of Computer Science and Engineering*, vol. 7, no. 3, pp. 1-11, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[16] Jonathan Katz, and Yehude Lindell, *Introduction to Modern Cryptography*, 2007. [CrossRef] [Google Scholar] [Publisher Link]

[17] Jagpreet Kaur, Shweta Lamba, and Preeti Saini, "Advanced Encryption Standards: Attacks and Current Research Trends," *International Conference on Advance Computing and Innovative Technologies in Engineering*, pp. 112-116, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[18] B. Akhil et al., "Light Weight Security Coding using PRESENT Algorithm for Cryptography Application," *SSRG International Journal of VLSI & Signal Processing*, vol. 7, no. 2, pp. 1-5, 2020. [CrossRef] [Publisher Link]

[19] Walid Bagga, and Refik Molva, "Policy Based Cryptography and Applications," *Proceedings of Financial Cryptography and Data Security*, vol. 3570, pp. 72–87, 2005. [CrossRef] [Google Scholar] [Publisher Link]

[20] Arun Pratap Singh, and Himanshu Pundir, "Secure File Storage on Cloud using Cryptography," *SSRG International Journal of Computer Science and Engineering*, vol. 7, no. 5, pp. 12-15, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[21] Fred Piper, "Recent Trends in Research in Cryptography and Security Mechanism in Cryptography," *Elsevier Science Ltd*, pp. 23–26, 2003.

[22] Ekta Agrawal, and Parashu Ram Pal, "A Secure and Fast Approach for Encryption and Decryption of Message Communication," *International Journal of Engineering Science and Computing*, vol. 7, no. 5, pp. 11481-11485, 2017. [Google Scholar] [Publisher Link]