International Journal of Scientific Research in Computer Science, Engineering and Information Technology
ISSN : 2456-3307 (www.ijsrcseit.com)
doi : https://doi.org/10.32628/CSEIT2173149

Merging Vernam Cipher stream and Rail Fence Algorithms and How Effective They are on IoT Devices

Adnan Adel Bitar*, Dr. V. Sujatha
Computer Science, CMS College of Science and Commerce, Coimbatore, Tamil Nadu, India

Article Info
Volume 7, Issue 3
Page Number: 686-691

Publication Issue :
May-June-2021

Article History
Accepted : 12 June 2021
Published : 20 June 2021

ABSTRACT

Encryption is the effective way to provide the needs of security and privacy. The performance of any encryption algorithm is one of the most important parameters if not the most one in encrypting data. Also, random access memory utilization plays an excellent role in ciphering plain texts. Speaking of standard simple encryption algorithms that most of them are weak and may not be safe to use them to cipher our data communication from any threat such as Caesar algorithm [2].However, they have good results in the parameters. Nevertheless, merging these simple algorithms could generate a more powerful algorithm that takes a very long time and excessive efforts to break it. Both standard algorithms "Vernam Cipher" and "Rail-Fence stream" merged to produce the "Railve" algorithm, which has great performance and consumes a small amount of RAM. The three algorithms are applied on two devices "a mobile phone and a laptop".
Keywords: Security, Vernam, Rail-Fence, encryption, performance, IoT.

I. INTRODUCTION

Science of making raw data as unfathomable data is called "encryption". And this procedure requires methods and mechanisms which are applied with specific or random keys [3]. Due to the development of internet and devices in the network, security plays an important role in data communication among different hardware devices [1]. And the encryption procedure makes the data traveling among devices secure and does not allow to interveners to steal these data. The encryption mechanism starts from the sender device where the readable text "plain text" is applied with a key in some methods to produce an incomprehensible form "ciphertext" which is sent to the receiver device where the cipher text is decrypted by the same key or not the same depending on the encryption type. Any encryption algorithm must be efficient and uncomplicated with no chance of mistakes. The performance of any encryption algorithm is one of the most important parameters if not the most one in encrypting data. Whereas the most famous algorithms have good performance, but there can be some hybrid algorithm that could give better performance. Moreover, random access memory "RAM" utilization plays an excellent role in ciphering plain texts.

As there are great encryption algorithms, there are also some bad old ones which could be enhanced and developed to produce better algorithms.

In this paper, the two encryption algorithms "Vernam Cipher" and "Rail-Fence cipher" are merged to produce the "Railve" algorithm. All the three encryption algorithms are tested on IoT devices. Performance and memory utilization are the parameters that are used to show how effective is the "Railve" algorithm.

II. METHODS AND MATERIAL

A. Material

❖ **Hardware:**

[1] HP Laptop:

A Laptop is a computer device containing high memory, fast processor, and various ports. HP 350 G1 laptop has a 15.6 Inches (39.62 cm) display for your daily needs. This laptop is powered by Intel Core i7-4600M (4th Gen) processor, coupled with 8 GB of RAM and has 1TB HDD storage at this price point. As far as the graphics card is concerned this notebook has an Intel HD 4400 graphics card to manage the graphical functions. It also has networking chips as wireless LAN and Bluetooth.

[2] Samsung S9 Mobile Phone:

The mobile device is considered as a small computer that has many features. S9 mobile has a processor called Exynos 9 that has octa-core (2.7 GHz, Quad-core, M2 Mongoose + 1.7 GHz, Quad-core, Cortex A53) which enables to process high tasks. And RAM of 4 GB that allows making the process faster. Furthermore, the network chips to connect to the internet and other devices by wireless and Bluetooth

❖ **Software**

All the encryption algorithms are executed using different software on each device to apply on the data. On the mobile phone, the software that is used is Pydroid3 and on the laptop, Spyder (Anaconda3) are used to execute the code of algorithms written in Python programming language. Nevertheless, the algorithm that produced from merging this algorithm has been done in Python.

B. Encryption Algorithms

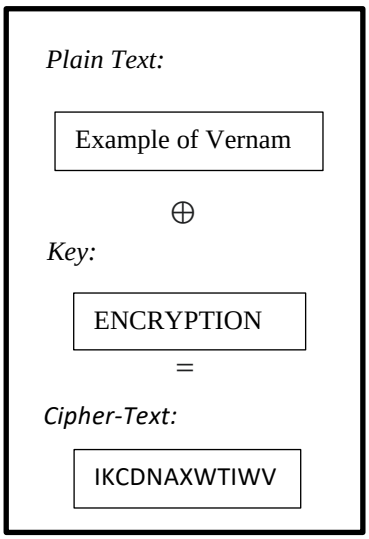
1. Vernam Cipher:

Vernam Cipher is a stream cipher that implements the encryption bit by bit. It is an encryption algorithm uses transposition technique to convert a plain text to a cipher text [7]. Vernam algorithm is using Boolean "exclusive or" (XOR) operation to apply the bits of the given key on the bits of the plain text. The function of XOR is represented by ⊕. The key is used to produce the cipher text as: Plaintext ⊕ Key = Ciphertext.

And the plain text is reproduced as:

Ciphertext ⊕ Key = Plaintext. [13].

Example:



2. Rail-Fence Cipher

Rail-Fence cipher is a stream cipher that implements the encryption bit by bit also. The plain text is formatted in a diagonal way downwards to issue the rails of a fictional fence. The implementation of Rail-Fence cipher depends on a key that is number of rows to split the plain text. For example, if the key is 3 and the plain text:

'WE ARE DISCOVERED. FLEE AT ONCE'.

The text will be written in 3 lines [14]:

W . . . E . . . C . . . R . . . L . . . T . . . E
. E . R . D . S . O . E . E . F . E . A . O . C .
. . A . . . I . . . V . . . D . . . E . . . N . .

To get: WECRLTEERDSOEEFEAOCAIVDEN

C. Method and the Proposed Work:

Both algorithms "Vernam" and "Rail-Fence" ciphers use the same cipher method which is called "stream" and this method depends on bit by bit stream. And they are compared and explained in detail [8]. Railve algorithm takes the plain text and applies Vernam algorithm first with a random key of 512 bits then the encrypted data is applied in Rail-Fence algorithm with a random key from 2 to 9 as standard and the key could go bigger if the file for encrypting goes bigger. For example, it can reach twenty lines as a key. So, Railve algorithm uses to keys ("Vernam key", "Rail-Fence key"). The strength of Railve algorithm is that the keys are truly random keys that make it unconditionally secure.

The diagram is explaining how Railve algorithm is processed. While an input string enters for Vernam encryption with the key string "ENCRYPTIONS", then the produced ciphertext is the input string for Rail-Fence algorithm with a random key "5" to produce the Rail-Fence ciphertext as shown in Figure I. As a whole process, the final output string is the cipher text of Railve algorithm.

So, clear as crystal that if a hacker tries to decipher the Railve cipher text to get Vernam Cipher text, he may get the right one but with no confirmation if it is correct, the hacker will find an ambiguous text, which leads him to nothing but confusion. So, key size of "256 bits" for Vernam and "9 rows" for Rail-Fence. However, key sizes may rise if needed to make better security [6]. For example: "512 bits" for Vernam and up to "20 rows" for Rail-Fence. Thus, increase of the key size of Rail-Fence requires the encrypted data to be large to execute successfully. Nevertheless, the accuracy of correctness for Railve algorithm is a hundred percent and that is proved by the done tests.

III. RESULTS AND DISCUSSION

The three cryptographic stream ciphers are implemented on a PC and a mobile phone. And the results are enlisted in tables and line graphs. The experiments are done on file sizes range from 1 KB to 128 KB. And all the results are average results ten times of implementation of the three ciphers.

Railve algorithm uses Vernam key size of 256 Bits and it is an automatic generated random key. And the Rail Fence key is a number from 2 to 9, selected randomly.

Whatever plain text size enters for implementation in Railve algorithm; the input equals the output, which means the plain text size, equals cipher-text size with an accuracy of a hundred percent.

The execution time in seconds and Memory utilization in KB for three-stream ciphers are shown in tables and figures. Table I

Comparing execution time among the three encryption algorithms on PC

File Size (KB)	Executing Time (Sec)		
	Vernam	Rail-Fence	Railve
1	0.002428329	0.007710971	0.00972263
2	0.005930214	0.015628686	0.02159794
4	0.012868214	0.026458157	0.03821605
8	0.0240908	0.056631157	0.07373092
16	0.052596057	0.102098186	0.13384314
32	0.093107143	0.373177371	0.26575999
64	0.1663192	0.420622329	0.4954769
128	0.326656029	1.024517357	1.04801471

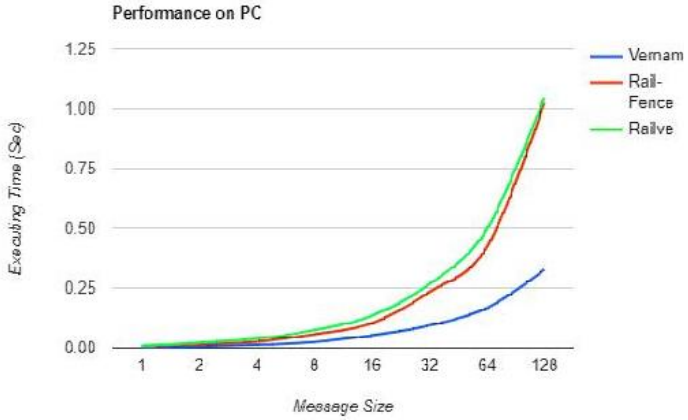


Figure 1. shows the executing times of three algorithms when applied on PC.

Table 1 and Figure 1 illustrate how speed is the implementation of three Ciphers; whereas Railve algorithm execution time approximately equals Rail-Fence execution time. But if Vernam and Rail-fence's execution times are added together, they would be more than Railve which is a combination of (Vernam and Rail-Fence) algorithms.

TABLE II

Comparing execution time among the three encryption algorithms on mobile phone			
File Size (KB)	**Execution Time (Sec)**		
	Vernam	**Rail Fence**	**Railve**
1	0.005158665	0.01030266	0.0144311
2	0.009826852	0.02080094	0.0248135
4	0.021405961	0.04233332	0.0529553
8	0.05235922	0.08290636	0.0960335
16	0.095435873	0.16267421	0.1904373
32	0.201269516	0.33117396	0.3772011
64	0.356282121	0.68645744	0.6635462
128	0.685798351	1.12328282	1.1590879

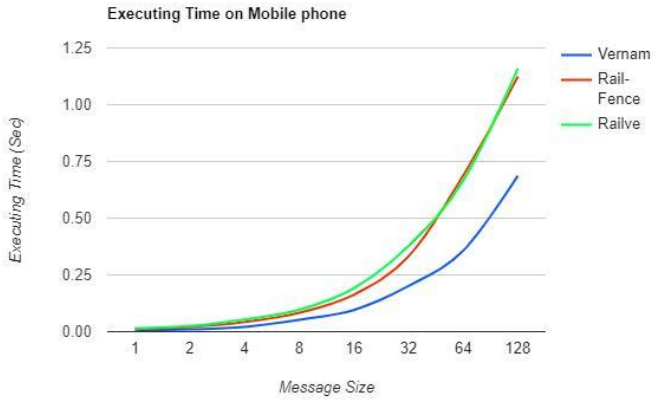


Figure 2. shows the executing times of three algorithms when applied on mobile phone.

Table 2 and Figure 2 illustrate how speed is the implementation of three Ciphers on the mobile phone; whereas Railve algorithm execution time approximately equals to Rail-Fence execution time. However, if Vernam and Railfence's execution times are added together, they would be more than Railve as in PC.

Comparing RAM utilization among the three encryption algorithms			
File Size (KB)	**Memory Utilization (KB)**		
	Vernam	**Railfence**	**Railve**
1	0.00	1	0.8
2	0.00	2	1.6
4	0.57	5.2	3.2
8	1.14	30.4	6.4
16	1.71	130	18.2
32	3.43	637.3	96.4
64	7.43	2078.2	1425.1
128	15.00	4158.4	3846.3

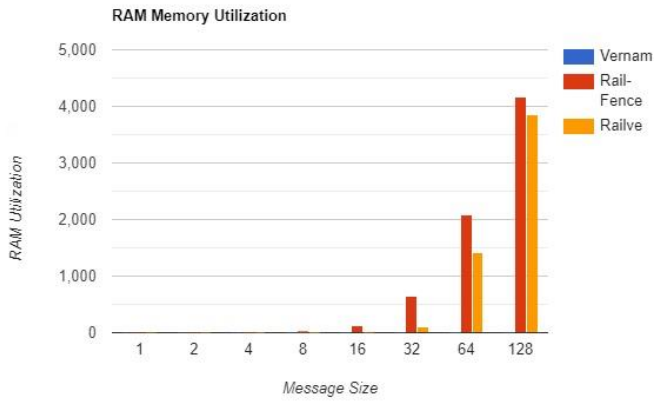


Figure 3. Shows RAM utilization (KB) of three algorithms when applied on PC.

Table 3 and Figure 3 illustrate how much RAM used by three algorithms. The results are from implementing algorithms on the PC. Nevertheless, after testing three algorithms on the mobile phone, the results were almost the same.

IV.CONCLUSION

To conclude, through this research work, as shown, Railve algorithm utilizes random access memory less than Rail-Fence algorithm. Nevertheless, Vernam Cipher uses 1KB for 128KB message size. Whilst, the execution speed of Railve algorithm is slower by 0.02 to 0.03 seconds approximately and this is not a value that matters when it comes for a better security.

It is clear that merging Vernam algorithm with Rail-Fence algorithm is showing great and more secure results and it produces and less amount of cipher text size comparing to other encryption algorithms which could benefit in making the transmission of data faster. Consequently, Railve algorithm is an excellent improvement comparing with base algorithms which it presents a better security and less RAM consumption.

V. FUTURE SCOPE

As future enhancement for Railve algorithm, Randomized Rail-Fence algorithm could be used instead of simple Rail-Fence to improve the security more. And the performance could be enhanced by optimizing the code of Railve algorithm.

VI. REFERENCES

[1]. Panda, M. "Performance analysis of encryption algorithms for security," 2016 International Conference on Signal Processing, Communication, Power and Embedded System (SCOPES), Paralakhemundi, 2016, pp. 278-284, doi: 10.1109/SCOPES.2016.7955835.

[2]. Gowda S, N. "Innovative enhancement of the Caesar cipher algorithm for cryptography," 2016 2nd International Conference on Advances in Computing, Communication, & Automation (ICACCA) (Fall), Bareilly, 2016, pp. 1-4, doi: 10.1109/ICACCAF.2016.7749010.

[3]. PETERS, K. "What Is Encryption?" https://www.investopedia.com/terms/e/encryption.asp. 2020

[4]. Jawad, Ahmad, D., S, Sandeep. (2012). "Implementation of One Time Pad Cipher with Rail Fence and Simple Columnar Transposition Cipher, for Achieving Data security," International Journal of Science and Research, vol. 3, no. 11, pp. 2415-2421.

[5]. Sengupta, N. (2018) "Security and Privacy at Cloud System". In: B. Mishra., H. Das., S. Dehuri ., Jagadev. (eds) Cloud Computing for Optimization: Foundations, Applications, and Challenges. Studies in Big Data, vol 39. Springer, Cham. https://doi.org/10.1007/978-3-319-73676-1_9

[6]. Siahaan, A, P, U. (2017, September 21). "Rail-Fence Cryptography in Securing Information". https://doi.org/10.31227/osf.io/h5jnz

[7]. https://web.archive.org/web/20121010011445/ https://www.nsa.gov/about/_files/cryptologic_heritage/publications/misc/tsec_kw26.pdf
[8]. https://web.archive.org/web/20110518125721/ http://www.simonsingh.net/The_Black_Chamber/railfence.html
[9]. Rajesh, S., Paul, V., Menon, VG., Khosravi, MR. (2019) "A Secure and Efficient Lightweight Symmetric Encryption Scheme for Transfer of Text Files between Embedded IoT Devices". Symmetry 11, Volume 293 - Number 2.
[10]. Banerjee, A., Hasan, M., Kafle, H. (2019) "Secure Cryptosystem Using Randomized Rail Fence Cipher for Mobile Devices." In: Arai K., Bhatia R., Kapoor S. (eds) Intelligent Computing. CompCom 2019. Advances in Intelligent Systems and Computing, vol 998. Springer, Cham. http://doi-org-443.webvpn.fjmu.edu.cn/10.1007/978-3-030-22868-2_52.
[11]. Singh, A., Nandal, A., Malik, S. (2012). "Implementation of caesar cipher with rail fence for enhancing data security." Int. J. Adv. Res. Comput. Sci. Softw. Eng. 2(12).
[12]. Udhayakumar, U., Murugaboopathi, G. (2020). To improve user key security and cloud user region-based resource scheduler using rail fence region-based load balancing algorithm. J Ambient Intell Human Computer. https://doi.org/10.1007/s12652-020-02152-2
[13]. https://en.wikipedia.org/wiki/Gilbert_Vernam..
[14]. https://en.wikipedia.org/wiki/Rail_fence_cipher

Cite this article as :

Adnan Adel Bitar, Dr. V. Sujatha, "Merging Vernam Cipher stream and Rail ?Fence Algorithms and How Effective They are on Internet of Things Devices", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 7, Issue 3, pp.686-691, May-June-2021. Available at doi : https://doi.org/10.32628/CSEIT2173149
Journal URL : https://ijsrcseit.com/CSEIT2173149