# Comparative Study on Vernam Cipher stream and Rail Fence Stream in IoT

Adnan Adel Bitar
PhD Scholar
CMS College of Science & Commerce
Coimbatore

V. Sujatha
Associate Professor
CMS College of Science & Commerce
Coimbatore

## ABSTRACT

Many encryption algorithms have been used to achieve the needed performance of securing data. And each encryption algorithm has its pros and cons. Due to the development of IoT in many areas and the continuous increase in its devices, securing data being transmitted became nigh on impossible.

## Keywords

Security, Vernam, Rail-Fence, encryption, performance, IoT

## 1. INTRODUCTION

Cryptography is the science of making plain text incomprehensible cipher text by applying mechanisms and key related to them to make the transmitted and stored data secure. Data grows rapidly, IDC forecasts the global datasphere will reach 175 Zettabytes by 2025. [1] This data increase demands improvement in data security architecture. There are uncountable processors used in various IoT devices, the common ones being used (laptop, mobile phone). Employing security mechanisms on such devices could lead to overload of processors and this would lead to power consumption or application delay. However, testing encryption algorithm on these devices and compare the results of parameters like efficiency and speed of execution and producing the cipher text. This paper introduces a comparative study on two standard stream algorithms “Vernam” and “Rail fence” by testing them on some IoT devices with different file sizes ranging from 1 Mb to 128 Mb and makes the needed charts to give brief statistics on both algorithms.

## 2. IOT DEVICES

### A. HP Laptop:

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 a Intel HD 4400 graphics card to manage the graphical functions. It also has networking chips as wireless LAN and Bluetooth.

### B. 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 to other devices by wireless and Bluetooth

## 3. CRYPTOGRAPHIC CIPHERS

World of technology is in continuous development and that affects the cryptographic techniques which used to ensure data is safe while transition. There are two kinds of cipher methods; stream and block methods. The following ciphers are standard stream ciphers “Rail-Fence cipher” and “Vernam Cipher”. Stream Ciphers proceed the encryption as stream of bits; which means the plain text goes through the encryption algorithm to extract the cipher text.

### 3.1 Rail-Fence

Rail Fence Cipher is a simple encryption algorithm which was invented in ancient time and used by the Greeks by a special tool. [2].

Rail Fence cipher is very weak cipher. A hacker simply has to try several depths "keys" until the correct one is found using brute force attack. It is easy to break because only one language is used. [3]

Rail-Fence cipher involves writing the plain text as separated letters on different upper and lower lines depending on an integer key from 2 to 9. The sequence of letters on the upper line is then followed by the sequence on the lower line, to create the final encrypted message. Security of Rail-Fence rises if the key goes beyond two lines to reach nine lines. To decipher a message encrypted using key, you will need to divide the message into halves depending on the key and write the second half below the first, so on. You can then read the message column by column. When deciphering any cipher text, it is crucial to know how many lines were used to encrypt the message. [4]

E.g. Let the plain text be:

I have to be at the university after two days

Key: 2. means two rows to divide and conquer

I a e o e t h u i e s t a t r w d y

h v t b a t e n v r i y f e t o a s

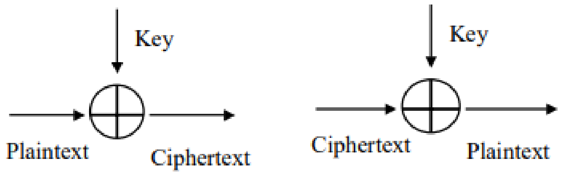
After encrypting:

Iaeoethuiestatrwdyhvtbatenvriyfetoas

### 3.2 Vernam Cipher

The Vernam Cipher is named after Gilbert Sandford Vernam, who invented the stream cipher. Vernam cipher was invented in 1917 and used over the years with a mechanism of 5 Bits. However, the modern use of Vernam Cipher implemented in IT field where the computers use 8 Bits words. But the main idea was the same where XOR operation is used.

Vernam is a symmetrical stream cipher in which the plaintext is combined with a random or pseudorandom stream of data to produce the cipher text by applying "exclusive or" XOR operation. [5]



The strength of this algorithm is that the key is a truly random key that makes it unconditionally secure. [6]

However, when Vernam Cipher was invented, the idea was to apply a key of same length of the plain text. Moreover, Shannon has proved that Vernam Cipher is unbreakable if the key is equal to the plain text. [7]

But as I have tested Vernam algorithm, a key of lesser size can be applied to produce a cipher text. And this is done in the experimental study.

E.g: Let the message: "be" and the key: [0100001] [0110011]

be: [1100010] [1100101]

[0100001] [0110011]

XOR

[1000011] [1010110] = CV

### 3.3 Experimental Results

The cryptographic stream ciphers both 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 Mb to 128 Mb. And all the results are average results of seven times of implementation of the two ciphers.

In Vernam Cipher, the key size is 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 the plain text size enters for implementation in both algorithms; the input equals to the output, which means the plain text size equals to cipher text size.

The execution time in seconds for both stream ciphers is shown in Table I and Table II.

**Table I Ciphers Executed on PC**

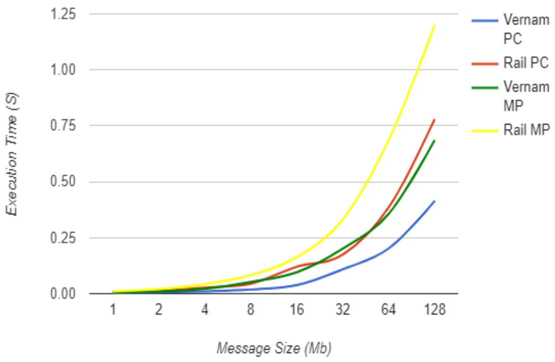
| File Size (Mb) | Execution Time (Sec) | |
|---|---|---|
| | Vernam | Rail Fence |
| 1 | 0.0025099 | 0.005490457 |
| 2 | 0.005451657 | 0.011839257 |
| 4 | 0.010047386 | 0.027101014 |
| 8 | 0.018417443 | 0.044710229 |
| 16 | 0.037858386 | 0.120119171 |
| 32 | 0.108451371 | 0.174332871 |
| 64 | 0.201774286 | 0.385300586 |
| 128 | 0.414523314 | 0.7790361 |

**Table II Ciphers Executed on Mobile Phone**

| File Size (Mb) | Execution Time (Sec) | |
|---|---|---|
| | Vernam | Rail Fence |
| 1 | 0.005158665 | 0.010302659 |
| 2 | 0.009826852 | 0.020800939 |
| 4 | 0.021405961 | 0.042333324 |
| 8 | 0.05235922 | 0.082906363 |
| 16 | 0.095435873 | 0.162674209 |
| 32 | 0.201269516 | 0.331173956 |
| 64 | 0.356282121 | 0.686457445 |
| 128 | 0.685798351 | 1.200432175 |

The tables I, II illustrates how speed is the implementation of Vernam Cipher; whereas Rail-Fence Cipher takes nearly twice the execution time of Vernam Cipher

Fig. 1 shows line graph that compares the execution time of both algorithms on Personal Computer “PC” and Mobile Phone “MP”. The difference is very clear that the PC takes half the time of the mobile phone approximately.



## 4. CONCLUSION

I have implemented two standard encryption algorithms on two different IoT devices and checked the speed of each algorithm on each device. Thus, the PC has the advantage over the mobile phone due to the better processor. Moreover, the memory consumption is stable before and after the execution of both ciphers, as a future enhancement; merging two standard algorithms could produce a high efficient algorithm that gives better throughput.

## 5. REFERENCES

[1] Seagate.com: The digitization of the world from edge to core, 2018

[2] http://www.crypto-it.net/eng/simple/rail-fence-cipher.html

[3] Dar. Jawad Ahmad and Sharma. Sandeep, “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 issue 11, 2014

[4] https://web.archive.org/web/20110518125721/http://www.simonsingh.net/The_Black_Chamber/railfence.html

[5] https://web.archive.org/web/20121010011445/https://www.nsa.gov/about/_files/cryptologic_heritage/publications/misc/tsec_kw26.pdf)

[6] Wang. Liyan, Li. Yonghua, Jia. Siqi, Gang. Jiatai,.” A stream cipher algorithm based on composite chaotic dynamical systems”. Journal of Dalian University of Technology, vol 52. 2012.

[7] Shannon. C.E, “Communication theory of secrecy systems”, Bell System Technical Journal, vol 28, no.4, pp. 656-715,1949.