ISSN XXXX XXXX © 2017 IJESC

Research Article Volume 7 Issue No.11

Protecting Information Through Cryptography

Ashish Agarwal
Software Engineer
Capgemini, Bangalore, India

Abstract:
The ever-increasing technologies with parallel advancements in the development of notorious attempts, to play with the integrity of the information, in the field of communication over the internet present the need for the equally enhancing security easures [1]. I have already referred to suggestions by means of several research papers being published so far related to our area of interest such as N-Prime R.S.A., magic rectangle, etc[2][3]. This paper would consist of a more enhanced technique to protect the transfer of information between two communicating parties.

Keywords: Cryptography, Key, Private Key, Public key, Asymmetric or Public Key Cryptography, Symmetric or Private Key Cryptography

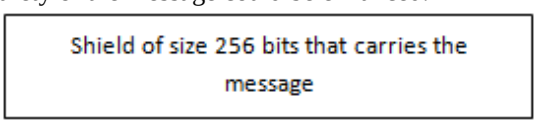
I. INTRODUCTION

Digitisation, as perceptible by its name, has taken its users to their needs with the single click on PC's or tap on smart phones irrespective of operating systems being functional on such platforms. Therefore, it has emerged as the field full of curiosities in terms of challenges and the ease of its usage for addressing one's needs. Most often we hear of cyber attacks called as digital attacks in slang that lead to some anticipation in its user's proclivity towards digital media. However, the front side of the coin looks panoramic but the other side equally tries to create bloom around the digital backbone. The significance of digitisation can be estimated by looking at world leaders promoting digitally supported platforms in their countries of which, India amongst others is the exemplifying spot on the globe. It is beyond doubt that social networking has brought world's corners more closely than ever as depicted by one of the social giant's logo i.e. Facebook, Instagram or LinkedIn. It is then worth pondering to the fact that there are insane threats attempted to foil the communication. Cryptography is one of those securing techniques that acts tool to the preservers and weapon against annihilating minds. Here is proposed a technique to the existing structure used hitherto and it can be unified with the symmetric key or private key cryptographic system.

II. DESCRIPTION

Cryptography is not new but the way it is implemented makes some difference(s). As it is defined being a technique that locks the information (or message) where the key (that is used to encrypt the message) plays a very crucial role in assuring the safety of locked stuff [1]. While rolling down through several researches, one can try to ensure the message's backend format in order to nullify daring attempts to tamper with the data. Below described the proposed method in points:

- The shield's size to cover up the information in the way to receiver's end can be fixed to 256 bits i.e. 2^8 so that the safety of the message could be enhanced.



- It is worth mentioning that the message has to be of 256 bits.
- In case the message, 'M' size is lesser than 256 bits i.e. $M< 2^8$, then appropriate special symbols will be appended in form of headers and trailers respectively in order to make message of 256 bits.
- Contrary, if message, 'M' comes to be greater than 256 bits i.e. $M>2^8$, then it will be broken into different shields of equal size i.e. 256 bits.

Note: The locking key (a symbol(s) that may be any number, alphabet, alphanumeric or special character(s)) will be same for all shields of message so generated due to restraint on transferable size of 256 bits.
It is important to highlight that already proposed techniques will be applicable to the aforementioned technique. The 2^n rule holds its significance unbiased but in more feasible way. Below explained is an example in support of three above-mentioned scenarios [5][6].

III. CASES

Note: In all following cases ignore square in([) and square out(]) brakets. They are just for representing the message

3.1. Case 1:

Suppose message, M=[My Best Friend's Name Is Albert.]
Now, message length is already 32bytes equivalent to 256 bits, therefore no header or trailer would be appended. Moreover, the median of fixed length message can be easily speculated thus applying 2^n rule to render it with wider base.

3.2. Case 2:

Suppose message, M= [My Best Friend's Name Is Albert. He is from USA.] Now message length is 48 bytes i.e. greater than threshold of 32bytes so it would be broken into two sub groups of 32bytes each as follows:
M_1=[My Best Friend's Name Is Albert.]
≡32bytes.
M_2=
[$$$$$$$$ He is from USA.@@@@@@@@]
≡32bytes.
It is to be noted that headers, '$' and trailers, '@' will be added alternatively initiating from headers respectively. It is also worth noticing that the value of n as calculated for 2^n rule in

the computation for key(s) will be calculated from original message, 'M' and remains same for sub messages, M_1&M_2.

3.3. Case 3:

Suppose message, M= My Friend is Andrew. Now message length is less than 32bytes so a header followed by trailer at end will be appended i.e.

[$$$$$$My Friend is Andrew.@@@@@@]

≡32bytes.

It is equally important to note that value of 'n' for applying 2^n rule would be calculated from original message, 'M'.

It may be inferred that message, 'M_2' in case 2 is an implication of case 3.

IV. CONCLUSION

The discussion covering detailed analysis of the safety measures and their application suggests concluding following points:

〉 2^n rule, proposed for computing the asymmetric keys, becomes more significant to put to use [2][3].

〉 The length of 256 bits fixed keeping in mind the communication bandwidth and feasibility of the network supporting business(s).

〉 Direct application of binary logic may be applied in implementing the idea [4].

〉 Security feature enhanced.

〉 However complex underlying structure gets, the overall feature of cryptographic system remains simplified.

〉 More robust in terms of mathematical calculations thus rendering faith and faster execution.

〉 Appending headers and trailers has to be done alternatively in case it is needed beginning from header.

〉 Greater reliability in terms of conducting business(s).

V. FUTURE ASPECT

However, examples from wide range of possibilities have been tried in taking into consideration for validating the proposed technique [7]. Despite it is open for challenges that may creep in and will be dealt with greater sense of trust. The different lengths as threshold may be tried supplemented with greater number of examples. Whatever method is put in use in order provide security to the communication, it is always a priority to preserve the basis of underlying principles and maintain the integrity of information thereby shielding the important information in its journey from sender's to receiver's end.

VI. REFERENCES

[1]. Neha Tyagi, Ashish Agarwal, Anurag Katiyar, Shubham Garg, Shudhanshu Yadav, "Protection of Key in Private Key Cryptography" paper published in "International Journal of Advanced Research", Volume 5, Issue 2, Feb 2017, DOI: 10.21474/IJAR01/3207.

[2]. Neha Tyagi, Ashish Agarwal, Anurag Katiyar, Shubham Garg, Shudhanshu Yadav, "Algorithm for Protection of Key in Private Key Cryptography" paper published in "International Journal of Engineering Research in Computer Science and Engineering", Volume 4, Issue 3, Mar 2017, DOI: 01.1617/ vol4/ iss3/pid39862.

[3]. Neha Tyagi, Ashish Agarwal, Anurag Katiyar, Shubham Garg, Shudhanshu Yadav, "Function Codes for Protection of Key in Private Key Cryptography" paper published in "Journal of Emerging Trends and Innovative Research", Volume 6, Issue 3, Jun 2017, DOI: 10.5281/zenodo.806860.

[4]. Neha Tyagi, Ashish Agarwal, Anurag Katiyar, Shubham Garg, Shudhanshu Yadav, "Hybrid Key Cryptography: A Tool for Security" paper published in "International Journal of Innovative Research in Science, Engineering and Technology", Volume 6, Issue 3, Mar 2017, DOI: 10.15680/ IJIRSET. 2017.0 603031.

[5]. Neha Tyagi, Ashish Agarwal, Anurag Katiyar, Shubham Garg, Shudhanshu Yadav, "Methods for Protection of Key in Private Key Cryptography" paper published in "International Journal of Innovative Research in Computer Science & Technology", Volume 5, Issue 2, Mar 2017, DOI: 10.21276/ ijircst.2017.5.2.5 .

[6]. Neha Tyagi, Ashish Agarwal, Anurag Katiyar, Shubham Garg, Shudhanshu Yadav, "Information Security: A Saga of Security Measures" paper published in "International Journal Of Engineering And Computer Science", Volume 6, Issue 3, Mar 2017, DOI: 10.18535/ijecs/v6i3.38.

[7]. Ashish Agarwal, Amit Kumar Gupta, "Enhanced Key Protection in Private Key Cryptography "paper published in "International Journal for Research in Applied Science & Engineering Technology", Volume 5, Issue 8, Aug 2017, DOI: 10.22214/ijraset.2017.8089.