

A Reliable Technique for Data Encryption Using Symmetric Approach

Priya Dagar¹ Mugdha Monga² Sachin Pannu³

^{1,2,3}Research Scholar

^{1,2,3}Department of computer Science Engineering

^{1,2,3}HMR Institute of Technology and Management, Delhi, India

Abstract— Today almost sixty percent of the world is on internet, with online data exchange becoming the most common way of transferring information with each other, it brings with itself a number of security risks to the said data. As per the Identity Theft Resource Centre, up until October, the number of publicly documented data breaches has already exceeded the total for 2020, putting 2021 on track to be a record year. To combat this pressing issue and achieve data security in the most efficient manner our research paper has proposed a model to achieve the same using encryption. It is one of the most reliable approaches to prevent the interference from intruder using a key. The symmetric approach uses a single key which is encrypted by the sender and later decrypted by the receiver. The key is generated using some basic operation such as decimal to binary conversion and vice versa, one's compliment, swapping, concatenation etc. This method encrypts the data and transforms it efficiently, making it difficult to be decoded by an unauthorized user. As it is a very convenient technique, it can easily be used in a number of modern applications to safely store and transfer sensitive data.

Keywords: Symmetric Approach, Cipher Text, Encryption, Security

I. INTRODUCTION

Encryption is an information security tactic or the art of concealing information in order to prevent unpermitted access to one's data. Data encryption accomplish confidentiality, integrity, authentication, and non-repudiation, among other information security goals.

We do this by using mathematical concepts and a set of rule-based calculations known as algorithms to modify messages in arbitrary ways so that it is completely unrecognizable to a third party.

Asymmetric and symmetric cryptographic key systems are the two types of cryptographic key systems. Everyone who has access to the data has the same key in a symmetric key system. To ensure privacy, the keys used to encrypt and decrypt messages must also be kept secret.

On the other hand, two keys are used in an asymmetric key system, also known as a public/private key system. The private key is kept secret, while the public key is made widely available to anyone who needs it.

We make use of the symmetric key systems in this paper.



II. FACTORS AFFECTING SYMMETRIC ENCRYPTION APPROACH

Symmetric encryption approach is used for various processes such as transactions through card. Hence it demands various aspects to be taken care to provide full-fledged security. The relevance of any algorithm in the world is dependent on a plethora of factors and so is this approach of symmetric encryption technique.

The aspects in its specification includes:

- 1) **Adaptability:** - Adaptability of an algorithm elucidates how good an algorithm to bear alterations due to some demands is.
- 2) **Certainty:** - It is the foremost necessary feature of an encryption algorithm. Moreover, it decides the robustness of an algorithm. Safety of a symmetric approach of encryption is based on the size of the key, i.e., the space occupied by the key.
- 3) **Computation time:** - The amount of time needed to execute the operation of encryption and decryption. It has to be kept to a bare minimum.
- 4) **Composition:** - Composition of an encryption algorithm determines its functioning and behaviour. For example- the kind of methodology and process one use. Basically, it includes all the properties and attributes of the key being employed.
- 5) **Configurability:** - The Configurability of an algorithm specifies its ability to execute and work on numerous sizes of data. It is one of the most indispensable features an encryption algorithm.

III. PROPOSED MODEL

A. Encryption Algorithm

- 1) Step 1 - Calculate the letter's ASCII value.
- 2) Step 2: Generate the binary value that corresponds to it. [Binary value should be 8 digits e.g., for decimal 32 binary number should be 00100000]
- 3) Step 3: Interchange the first digit with last, second with second last, third with third last and so on.
- 4) Step 4: Divide 8 bits into two parts: element-1 is the first four digits, and element-2 is the second four digits.
- 5) Step 5: Append both the element 1 and element 2 with 4 zeroes in the Least Significant Bit (LSB).
- 6) Step 6: Now these two 8-bit digits will become element 1 and element 2 respectively.
- 7) Step 7: Convert element 1 and element 2 into their respective decimal values.
- 8) Step 8: Merge decimal value of element 1 and element 2 and we will get the cypher text.

B. Decryption Algorithm

- 1) Step 1: Take the cypher text and remove the 4 zeroes in Least Significant Bit (LSB) from element 1 and element 2 respectively.
- 2) Step 2: Now these 4-bit numbers (without zeroes) become element 1 and element 2 respectively.
- 3) Step 3: Generate a new 8-bit number by appending element 1 and element 2.
- 4) Step 4: Interchange the first digit with last, second with second last, third with third last and so on.
- 5) Step 5: After interchanging the original is generated back.

C. For example-

For encryption, if we take the letter ‘A’ generating the ASCII value 65. Then generate its corresponding binary value which is 01000001.

Further, Construct the 1’s compliment of the binary number i.e., 10111110 and now interchange the first digit with last, second with second last, third with third last and so on which generates 01111101.

Furthermore, divide this 8-bit binary number into two halves i.e., 0111 as element 1 and 1101 as element 2. New element 1 becomes 01110000 and new element 2 becomes 11010000.

Lastly, Convert both numbers into decimal form i.e., 112 and 208 respectively. Now merge these two numbers together which forms 112208.

If any of the element 1 or element 2 has less than three digits then add 0’s in its MSB accordingly to make it a 3-digit number. While in decryption we have to do the above steps in reverse order.

Firstly, divide the decimal into two 3 digits decimal number which are named as element 1 and element 2.

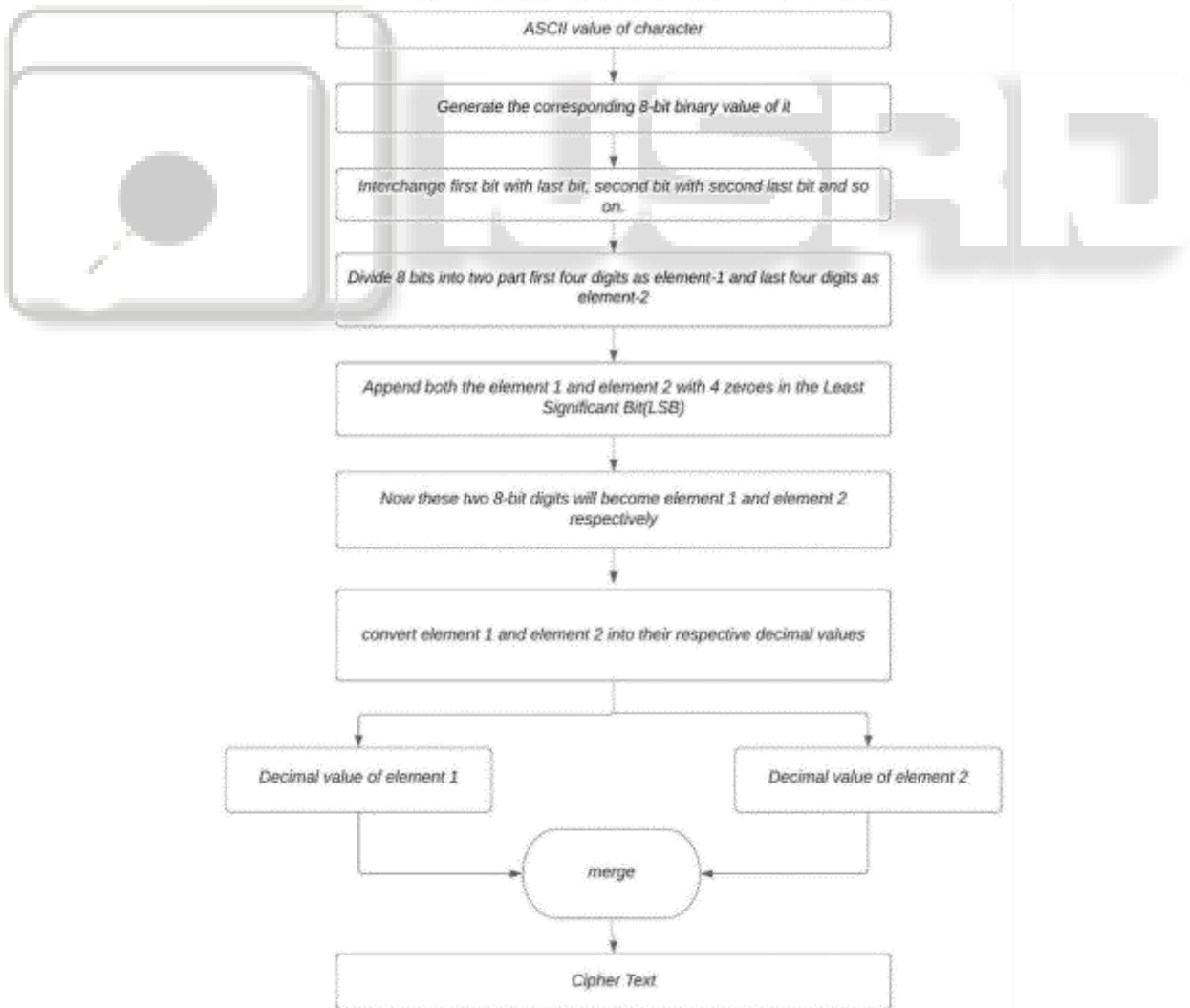
Element 1: - 112 and Element 2: - 208.

Now generate the 8-digit binary form of the element 1 and element 2. Therefore element 1 becomes 01110000 and element 2 becomes 11010000.

Then remove the four zeros from the LSB making element 1 as 0111 and element 2 as 1101. Further, append element 2 with element 1 which generates the 8-bit binary number as 01111101.

Now interchange the first digit with last, second with second last, third with third last and so on which becomes 10111110.

Lastly, compliment this binary number and finally the binary number formed is 01000001. Finally, compute the ASCII value of the corresponding binary number and hence the ASCII character got decoded which is 65. Hence represents “A”.



Architecture and flow of proposed algorithm.

IV. LITERATURE REVIEW

Some relevant research on Encryption techniques, their outputs and security potential are as follows:

In 2018 Priasnyomo Prima Santoso et al “Systematic literature review: comparison study of symmetric key and asymmetric key algorithm”. They analysed and compared both the encryption algorithm techniques and concluded that symmetric key algorithm is considered good in speed and power consumption while asymmetric key algorithm in terms of tunability.

In 2011 Srinivasarao, Dadi A et al. “Analysing the Superlative Symmetric Cryptographic Encryption Algorithm (ASCEA).” proposed in the case of using the key the Blowfish has the best use where the code is unbreakable it was proposed that Blowfish is significantly efficient for preventing data misuse, followed by AES and RC6.

In 2019 Mandal, Dr & Deepti, A R. et al “A Review Paper on Encryption Techniques.” Mentioned Blowfish’s security lies in its variable key size (128-448 bits) providing a high level of security. Blowfish is resistant to various attacks because the key consists of several spherical keys that are significantly independent, making such attacks exceptionally difficult or unattainable.

"A Study of Encryption Algorithms AES, DES, and RSA for Security" was proposed by Perna Mahajanet in 2013. They used three encryption algorithms, which are AES, DES, and RSA, and compared their performance to that of other encryption techniques which are based on of encryption and decryption time. They also show the results of effectiveness analyses for each algorithm. Based on the text files used and the results of the experiment.

In 2014 Anjula Gupta et al. proposed “Cryptography Algorithms: A Review”. They did a analysis on existing encryption techniques to promote the performance of the encryption methods. To summarise, they used unique ID in all of their techniques. They looked at a lot of papers and discovered that BLOWFISH has a higher throughput and lowest power consumption as compared to all other symmetric algorithms. BLOWFISH has the lowest power consumption.

"Efficient Encryption Techniques in Cryptography Better Security Enhancement" was proposed by Reema Gupta in 2014. They proposed an investigation into encryption techniques, as well as their limitations and procedures. For encryption, Huffman coding and B2G, G2B are used. They also discussed various transpositional techniques like Simple columnar, simple row, Route cipher, transposition.

V. EXPERIMENTAL ANALYSIS

For experimental analysis, the simple text message including text only is used.

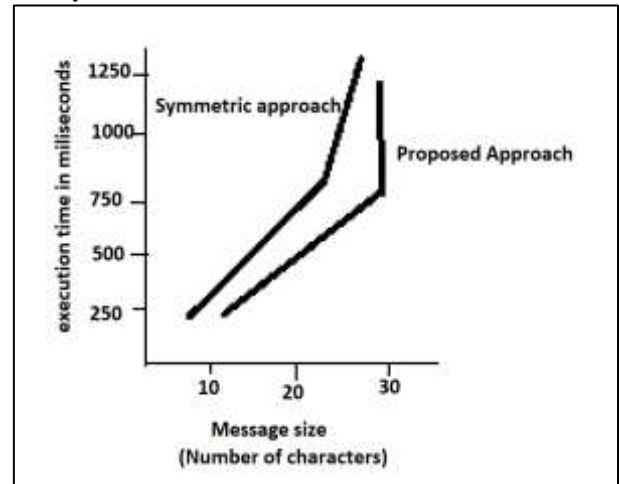


Fig. 1: Comparisons graph for encryption using symmetric and proposed approach

Figure 1 shows the comparison graph between the message size and execution time of symmetric approach and proposed approach.

Approach	Key size (in bytes)
Symmetric Approach	128
Proposed Approach	64

Table 1: Time required for execution on file

Table 1 shows the key size in bytes for encryption of symmetric approach and proposed method. Moreover, Figure 2 gives the graphical representation of table 1.

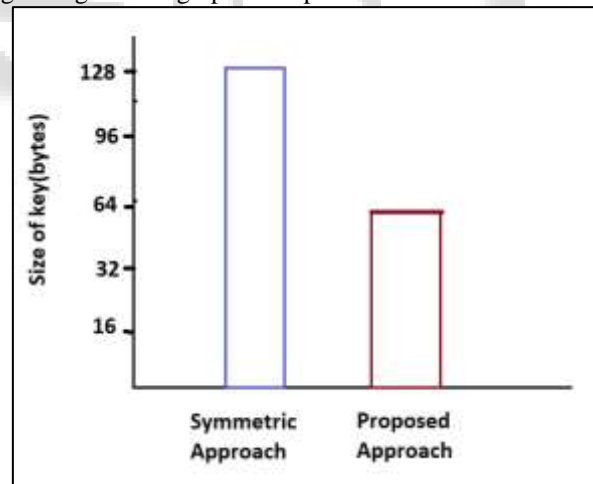


Fig. 2: key size

VI. CONCLUSION

The proposed algorithm mentioned above can thus be used to encrypt small data into something unreadable. This method makes use of small calculations and simple methods of transformation to convert the required raw data into its encrypted form thus can be implemented very easily even in the low power systems. This can be used to make the task of encryption more efficient, easy and resourceful. As of now this algorithm can only be used for numerical values and in the future, we hope to extend it to characters and special characters as well.

REFERENCES

- [1] William “Cryptography and Network Security Principles and Practice”, Fifth Edition, Pearson Education, Prentice Hall, 2011.
- [2] Schneier B, “Applied Cryptography”, John Wiley & Sons Publication, New York, 1994.
- [3] A. Kahate “Computer and Network Security” 2nd Edition, Tata Mc-Graw – hill Publisher ltd, 2011.
- [4] Ayushi “A Symmetric Key Cryptographic Algorithm” International Journal of Computer Applications (IJCA) ISSN: 0975-8887) Vol. 1 – No. 15 February 2010. Available: <http://www.ijcaonline.org/journal/number15/pxc387502.pdf>
- [5] Suyash Verma, Rajnish Choubey, Roopali soni “An Efficient Developed New Symmetric Key Cryptography Algorithm for Information Security” International Journal of Emerging Technology and Advanced Engineering Website: www.ijetae.com (ISSN 2250-2459, Volume 2, Issue 7, July 2012) Available: http://www.ijetae.com/files/Volume2_Issue7/IJETAE_0712_03.pdf
- [6] Prerna Mahajan & Abhishek Sachdeva “A Study of Encryption Algorithms AES, DES and RSA for Security” Global Journal of Computer Science and Technology Network, Web & Security Volume 13 Issue 15 Version 1.0 Year 2013 Type: Double Blind Peer Reviewed International Research Journal Publisher: Global Journals Inc. (USA) Online ISSN: 0975-4172 & Print ISSN: 0975-4350 Available: https://globaljournals.org/GJCST_Volume13/4-A-Study-of-Encryption-Algorithms.pdf
- [7] Anjula Gupta Navpreet Kaur Walia” Cryptography Algorithms: A Review” International Journal of Engineering Development and Research 2014 IJEDR | Volume 2, Issue 2 | ISSN: 2321-9939 Available: https://www.ijedr.org/papers/IJEDR_1402064.pdf
- [8] Reema Gupta “Efficient Encryption Techniques in Cryptography Better Security Enhancement” Volume 4, Issue 5, May 2014 ISSN: 2277 128X International Journal of Advanced Research in Computer Science and Software Engineering Research Paper Available online at: www.ijarcsse.com Available: https://www.ijarcsse.com/docs/papers/Volume_4/5_May2014/V4I5-0450.pdf
- [9] Abhishek Joshi a*, Mohammad Wazid b, R. H. Goudarc “An Efficient Cryptographic Scheme for Text Message Protection against Brute Force and Cryptanalytic Attacks” Available online at www.sciencedirect.com International Conference on Intelligent Computing, Communication & Convergence (ICCC-2014) Conference Organized by Interscience Institute of Management and Technology, Bhubaneswar, Odisha, India Available: <http://www.sciencedirect.com/science/article/pii/S1877050915007036>
- [10] Ashraf Odeh, Shadi R. Masadeh, Ahmad Azzazi “A Performance Evaluation of Common Encryption Techniques with Secure Watermark System (SWS)” International Journal of Network Security & Its Applications (IJNSA) Vol.7, No.3, May 2015. Available: <http://www.ircse.org/journal/nsa/7315nsa03.pdf>