JOURNAL OF CRITICAL REVIEWS

ISSN- 2394-5125 VOL 7, ISSUE 15, 2020

CRYPTOGRAPHY WITH PERMADD AND DISTANCE DIFFERENCE ALGORITHMS

SATHYA SANKARAN[1], Dr.RAJKUMAR RAJASEKARAN[2]

[1,2] School of Computer Science and Engineering, Vellore Institute of Technology, Vellore, India
[1]sathyamtvps@gmail.com, [2]vitrajkumar@gmail.com

ABSTRACT:

Cryptography is a method used to protect confidential data when it is sent over a network. In this work, a symmetric key encryption method, PERMADD, is suggested in which there are n levels of permutation and addition on the input data. Random numbers are generated which are used as key for permutation and addition. The input data is permuted in which each number in the input data is shifted to a random position that is given by the random number generator. Likewise, values are added to the permuted values in the position generated by the random number generator. Distance difference algorithm is a symmetric key algorithm used to encrypt the key, which are the random numbers generated and sent to the decryption module.

KEY WORDS: Distance Difference Algorithm, PERMADD, Encryption Decryption

I. INTRODUCTION

It is required to send confidential data such as medical records from one location to another that is from one doctor to another over the internet. It is possible that this data may be intercepted by hackers. They might cause changes to the records which may modify the diagnosis, treatment etc. To avoid this, the data is encrypted and sent to the next location. At the receiving end, the encrypted data is decrypted. In this work, PERMADD, there are several levels of permutation, addition stages which does permutation of data and addition of values to the permitted data. Permutation is done on the ASCII values of the data by shifting each number to a position given by a random number generator. Addition of values starting from 1 and increasing by 1 is done to the numbers at the position generated by the random number generator. Distance difference algorithm is used to encrypt and compress the list of random numbers generated, that is the key for PERMADD, and send it to the receiving end for decryption.

II. LITERATURE REVIEW

In [2] two algorithms DYNCBASE and DIGTBASE is proposed. They combine a list of ASCII values for the input text and generate large numbers on which Elliptic curve encryption is applied at the sender end. Decryption is done at the receiving end. In [3] both hybrid cryptography and steganography is applied. AES is used to encrypt the input message. The symmetric key used for encryption is further encrypted using public key of RSA. The message is used to generate a hash value which is encrypted by public of RSA to generate a digital signature. This digital signature is used to check integrity of the message at the receiving end. All the encrypted files are combined to form a complete message which has been embedded using the steganography method LSB. In [4] security is achieved by converting printable characters into non printable characters. This is achieved by conversion on ASCII cyclic mathematical function and radix conversion on the message multiple times. In [5] the key is generated automatically to encrypt the data. The automatically generated data is converted into a string and it is used for encryption and decryption. [6] shows the possibility of a neural network to learn neural cryptography.[7] deals with encrypting bangla script and it was found that Blowfish and Lempel-Ziv-Welch are suitable for encryption decryption. In [8] focus is on secure computation, which does computation on encrypted data. In [9]visual cryptography, an image is divided into several shares and sent to the recipient. In a k-out-of-n scheme k shares are sent to the receiver and the stacking the k shares gives the original image at the receiver. In [10] data is embedded in images using improved histogram shifting method. Reversible data hiding is done in the image which is then encrypted.

ISSN- 2394-5125 VOL 7, ISSUE 15, 2020

III. PROPOSED METHODOLOGY

PERMADD Encryption Decryption

The input data is converted into ASCII. The encryption module consists of N layers of permutation and addition components. N may be an integer such as 5 or 10 depending upon the complexity in the encryption required. Each level has a permutation component that take as input the input data in ASCII (in the first level) or the output of the previous level(other levels). It also takes as input the random numbers generated by a random number generator. If the 1st random number generated is 48, the first ASCII value in the input data is shifted to the 48th position. If the 2nd random number generated is 26, the 2nd ASCII value is shifted to the 26th position. Likewise, for all other numbers. The addition component takes the output of the permutation component as input along with the random numbers generated by the random number generator. If the 1st random number generated is 35,1 is added to the number at the position 35. If the 2nd random number generated is 52, then 2 is added to the number at the position 52. Likewise for all numbers that are input to the addition component. Each level is made up of such a combination of permutation and addition components.

Decryption is achieved by using the random numbers used for permutation or addition at a given level. The random numbers, key of PERMADD are obtained by decryption module of distance difference algorithm. The decryption is done as follows. If the 1st random number generated for addition component of the last level is 32, a value of 1 is subtracted from the 32nd number is the addition component. If the 2nd random number generated is 12, a value of 2 is subtracted from the 12th number in the addition component, and so on. Once the addition component has been processed, the numbers obtained by it is given as input to the permutation component of the same level. In the permutation component, if the 1st number generated by the decryption module of distance difference algorithm is 45, the number at position 45 is shifted to position 1. If the 2nd number generated by decryption module of distance difference algorithm is 87, the number from position 87 is shifted to position 2 and so on. The output of permutation component is given as input to the addition component of the previous level and the process is repeated till level 1.

Encryption and Decryption of key using Distance-Difference Algorithm

The key is encrypted using a symmetric key cryptographic algorithm, distance difference algorithm. The random numbers generated in each stage for permutation and addition are mathematically squeezed separately into a small set of numbers by using the distance difference algorithm discussed in [1]. The distance difference algorithm groups the input numbers into blocks of 100 numbers. The difference between the 1st and 101st number is found and added as the 1st number in the next level. The difference between the 2nd number and the 102nd numbers is found and added as the 2ndnumber in the next level and so on. Likewise the difference between the 101st number and 201st number is found and added to the next level. So also the difference between 201st and 301st, 202nd and 302nd and so on. A new set of numbers will emerge in the next level, level 2 by performing the above. The same operation of finding differences is performed on level 2, which results in numbers in level 3 and so on. This process is repeated until 100 numbers are reached. This set of numbers is sent to the receiving end along with the starting number of the sequence at each level so that the original random numbers may be generated by the process of addition in reverse of the difference operation.

IV. ADVANTAGES

Since a random number is generated for every permutation and addition operation, PERMADD is an efficient algorithm similar to one time pad, but the operations are different. Distance difference algorithm reduces the key to a minimum of 100 numbers. So it does not take much space for the key. It strengthens PERMADD by encrypting and decrypting its key.

V. CONCLUSION

PERMADD uses permutation and addition operations and the number of levels required is at the choice of the cryptanalyst wanting to use it. The operations are simple but efficient. Distance difference algorithm is suitable for encrypting the key of PERMADD.

ISSN- 2394-5125 VOL 7, ISSUE 15, 2020

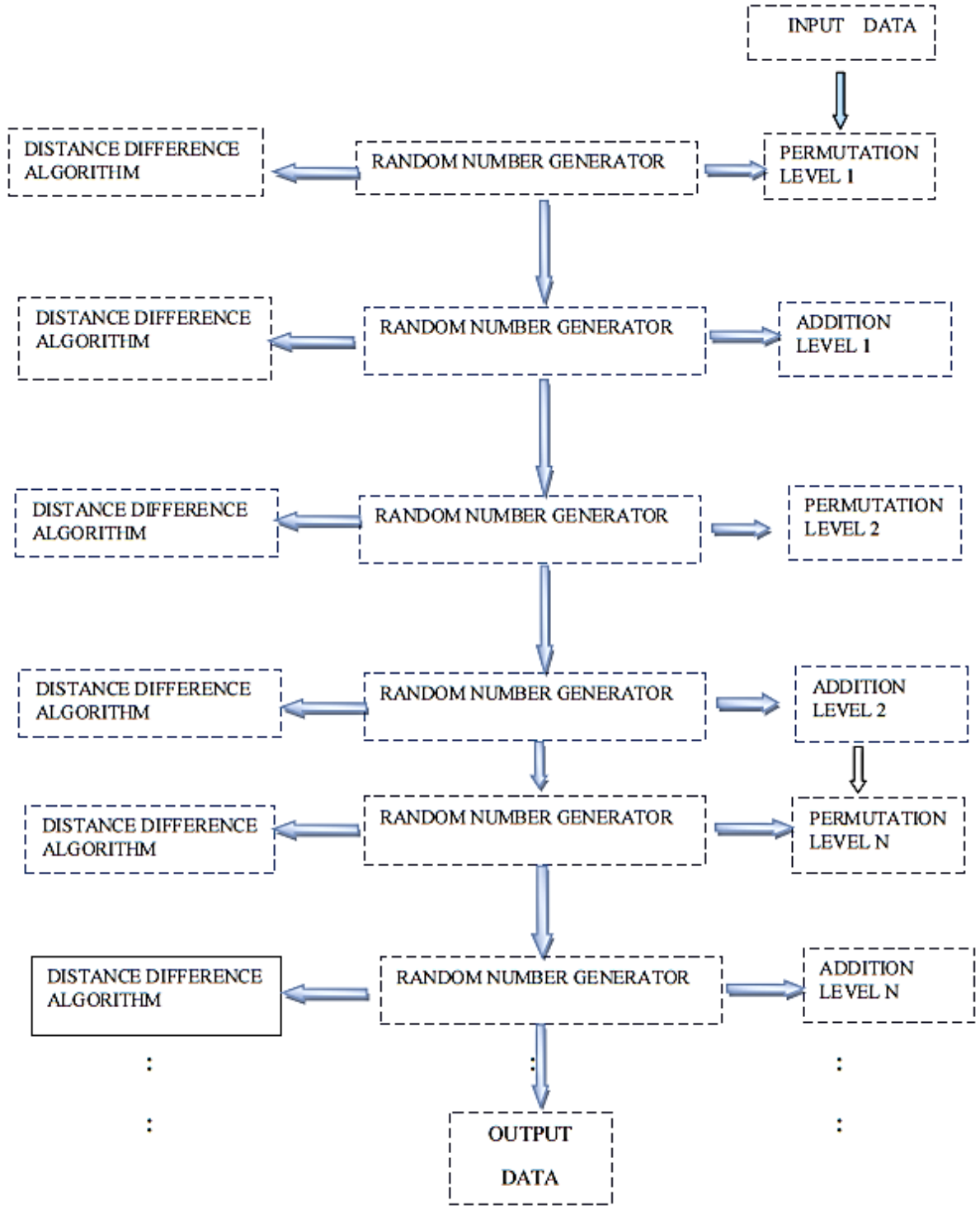

Figure 1. PERMADD Encryption

REFERENCES

1. Sankaran, S., & Rajasekaran, R.(2017,February). Secured Medical Data Storage over Cloud for Comprehensive Treatment. In 2017 *Second International Conference on Recent Trends and Challenges in Computational Models (ICRTCCM*) (pp. 257-262). IEEE
2. Das. P., & Giri, C. (2018, December). An Efficient Method for text Encryption using Elliptic Curve Cryptography. In *2018 IEEE 8th International Advance Computing Conference (IACC)* (pp. 96-101). IEEE.

3. Biswas, C., Gupta, U. D., & Haque, M.M. (2019, February). An efficient algorithm for confidentiality, integrity and authentication using hybrid cryptography and steganography. *In 2019 International Conference on Electrical, Computer and Communication Engineering (ECCE)* (pp. 1-5). IEEE.
4. Krishna, Y.S.R. (2015). Cryptographic algorithm based on ASCII conversion and radix functions. *International Journal of Scientific & Engineering Research*, 6(11).
5. Sultana, R., & Kumari, T. M. (2016). An ASCII value based optimized text data encryption system. *International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering* , 5(8).
6. Zhu, YP., Vargas, D.V., & Sakurai,K. (2018, November). Neural Cryptography Based on the Topology Evolving Neural Networks. In *2018 Sixth International Symposium on Computing and Networking Workshops (CANDARW)* (pp.472-478). IEEE.
7. Akhter, S., & Chowdhury, M.B. (2019, January). Bangla and English text cryptography based on modified blowfish and Lempel-Ziv-Welch algorithm to minimize execution time. In *2019 International Conference on Robotics, Electrical and Signal Processing Techniques (ICREST)* (pp. 96-101). IEEE.
8. Chida, K., Morohashi, G., Fuji, H., Magata, F., Fujimura, A., Hamada, K., … & Uamamoto, R. (2014). Implementation and evaluation of an efficient secure computation system using 'R' for healthcare statistics. Journal *of the American Medical Informatics Association, 21(e2)*, e326-e331.
9. Basavegowda, R., & Seenappa, S. (2013, April). Electronic medical report security using visual secret sharing scheme. In 2013 *UKSim 15th International Conference on Computer Modelling and Simulation* (pp. 78-83). IEEE.
10. Yang, Y., Xiao, X., Cai, X., & Zhang, W. (2019). A Secure and High Visual-Quality Framework for Medical Images by Contrast-Enhancement Reversible Data Hiding and Homomorphic Encryption. *IEEE Access, 7*, 96900-96911.