File Encryption and Decryption Using Cryptanalysis

Sreelekshmi S [1]
Department of Computer Science & Engineering
Mangalam College of Engineering ,
Ettumanoor, India
ssreelekshmi10@gmail.com

Tinu Thomas [2]
Department of Computer Science & Engineering
Mangalam College of Engineering
Ettumanoor, India
tinu.thomas@mangalm.in

***Abstract*—**
The process of converting the initial text communication into an ambiguous form, as well as in reverse, is known as cryptography. It is the process of concealing data and transmitting it in an appropriate format so that only authorized individuals may access and use it. Data security for consumers is mostly achieved through the use of cryptographic processes, which protect data against theft or transformation. This paper defends the use of Sequences of DNA (Deoxyribonucleic Acid) used for encryption and decryption. To encrypt the communication, two intermediary steps in this procedure are used: perception of binary-coded form and generation of arbitrary keys. For the purposes of encryption and decryption, the sender and receiver should establish a shared key. The sequence is more secure thanks to the shared key. This paper examines both the process. And also we have included three level of security. We have added image steganography with encryption using RSA before DNA encryption which makes the data more secured from the hijackers.

Keywords*— *DNA Encryption and Decryption techniques, Image Steganography, RSA encryption and Decryption

Introduction

Due to the effective expansion of transmission applications, data security has become increasingly important in communication systems. The process of converting the initial text message into an ambiguous form is known as encryption. Decryption is the process of returning encrypted data to its initial condition. The process of encrypting and decrypting data is known as cryptography, commonly referred to as cryptology. Data is encrypted on the sender side and decrypted on the receiver side before being sent over the network. Based on the key-value pair and the cryptographic method that is used to encrypt and decrypt the provided results, the current cryptographic technique can safely encrypt the data. The numerical key that is employed for both encryption and decryption.

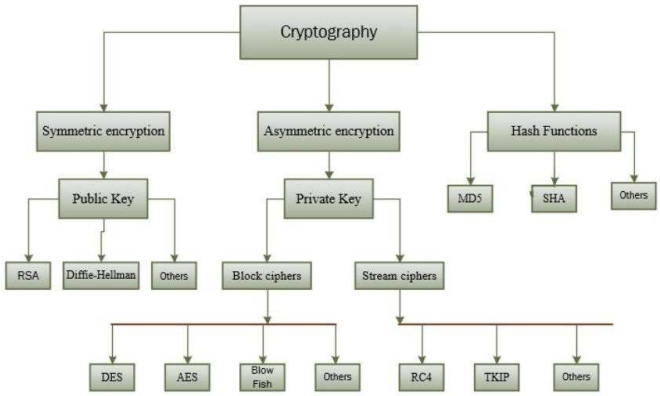

Fig: 1: Different Types of Cryptography

We have used three different techniques to make the data more secured and confidential. The RSA Technique make the data more secured using a key. And hiding the text in image makes the hackers more complicated from hijacking. Above all these, For a third level of security , we have used DNA encryption technique also.

CHALLENGES

Nowadays data access has been easier but more challenges occur in the acquisition and processing of data. Longer DNA might be encrypted for greater security. Sequencing takes longer. Security is entirely dependent on the key. Due to the length of the keys, asymmetric cryptography is much slower than symmetric key encryption. All these are the current challenges in the published papers. One time padding is also another method in which the decrypt message uses a codebook which may not be possible for all messages.

RELATED WORKS

Based on the different techniques used along the past years it was found an accurate method is less in the field. So combination of different techniques together can make the data more secured.

In [1], Pushpa. Introduced a DNA synthesis, using DNA digital coding and PCR amplification. Prevent attack from a possible word as PCR primers. The complexity of Biological scheme and cryptography computing provide a double security safeguards for the scheme. Cost of encryption scheme was low but he faced some challenges like Security can depend only on

decryption key. The encryption scheme is still far away being a perfect scheme.

In [2], Chen Jie mentioned symmetric key method where he has used one time pad and DNA molecular structure methodology. Storing large amount of data in compact volume and Massive parallel processing capabilities of biomolecular computation were his contribution to this paper but there were some research gap also they are the message decryption was done using codebook but it was difficult to send messages which was not in codebook.

In [10], Nandhini Subramanian has worked on image steganography, the main goal is to analyze and explain the various learning methods applied to image steganography. An embedding algorithm is utilized to create the container stegano image from the inputs of the cover image and secret information. The stegano image is used as input by the extraction algorithm to retrieve the embedded secret information.

In [6], Deepak and team were working on one time padding using symmetric key. They found that any change in the text cipher is easily detectable and also can remove the deficiency in the scheme of steganography and cryptography but the main research gap was that all security depends on the key.

In[12], Yunpeng Zhang and gang used DNA Fragmentation methodology and contributed that length of cipher is secured and short but since the length was short it was easy for an attacker to hack easily.

PROPOSED METHODOLOGY

A. Framework for file encryption and decryption using multiple technologies

The proposed system has three level of encryption techniques used for the higher security of data. The different techniques used in the system are image steganography, RSA based encryption and DNA based encryption. The text file is first converted into ASCII and then we binaries the ASCII. The binarised value is used for image steganography where the value is made hidden using an image. The output from steganography is then encrypted using RSA algorithm using a public key and then encrypted file is again processed with DNA encryption which gives a genomic data. And in the decryption side the vice versa of each of the techniques happens and finally we obtain the same text file.

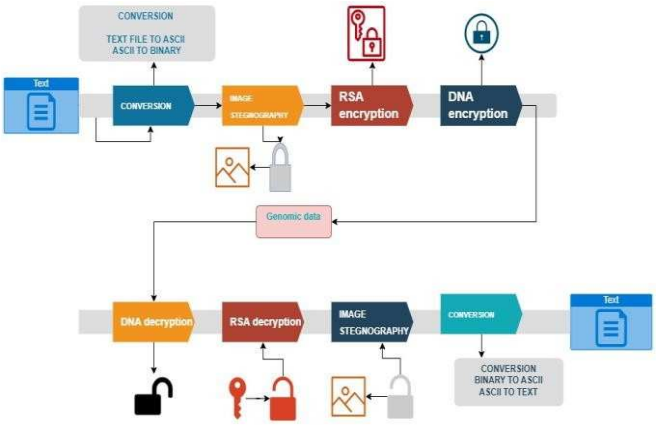

Fig:2: proposed system

CONCLUSION

In the recent years, DNA Encryption techniques have made more secured form of data transfer.

From the observation of earlier papers, we could make the data security more complex by adding more techniques to the DNA so that no hackers can extract the data easily.In this paper, different methods used in file encryption and decryption were discussed. Different encryption techniques such as AES, RSA, and CIPHER were considered here. Out of the various methods this paper talks about the combination of multiple techniques in a single program to make more security for data. Hence this paper helps to send data in a safer way compared to all the older methods.

In order to keep the data safe from attackers, the combinations of encryption techniques are used in this paper. DNA algorithm is more efficient because it can store huge amount of data. RSA algorithm use key for encryption and decryption therefore making the data more secured from attackers and also image steganography helps data hide inside a cover image which may confuse the attacker from attacking. Hence we could provide a three level security for the data or textual file. In the future, we could use a random key for DNA algorithm which makes the code more complex and no one can easily hack the data. We can also add a hashing technique inside image steganography as another level of security in the future.

ACKNOWLEDGMENT

The author would like to thank all the anonymous reviewers for their helpful suggestions and comments that will help in improving this paper.

REFERENCES

[1] Pushpa, B. R. (2020). A new technique for data encryption using DNA sequence. 2020 International Conference on Intelligent Computing and Control (I2C2). doi:10.1109/i2c2.2020.8321834

[2] Chen Jie, “A DNA-based bio molecular cryptography design,” Proceedings of IEEE International Symposium, Vol. 3, pp. III-822, (2003). [3]Kumar, D., & Singh, S. (2011). Secret data writing using DNA sequences. 2011 International Conference on Emerging Trends in Networks and Computer Communications (ETNCC). doi:10.1109/etncc.2011.6255930

[4] Menaka, K. (2014). Message Encryption Using DNA Sequences. 2014 World Congress on Computing and Communication Technologies. doi:10.1109/wccct.2014.35

[5] Priya, S. V. K., & Saritha, S. J. (2017). A robust technique to generate unique code DNA sequence. 2017 International Conference on Energy, Communication, Data Analytics and Soft Computing (ICECDS). doi:10.1109/icecds.2017.8390178

[6] Deepak Kumar, and Shailendra Singh, "Secret data writing using DNA sequences," In Emerging Trends in Networks and Computer Communications (ETNCC), IEEE International Conference on, pp. 402-40, (2011).

[7] Wang Zhong, Zhy Yu, “Index-based symmetric DNA encryption algorithm”. Image and Signal Processing (CISP),

2011 4th International congress on image and signal processing, 15-17 oct. (2011).

[8]J. D Watson, F. H. C. Crick, “A structure for deoxyribose nucleic acid”,Nature, vol. 25, pp. 737-738, 1953.

[9] William Stallings. Cryptography and Network Security, Principles andPractices, Forth Edition, Prarson Education, 2008.

[10] Nandhini Subramanian , Somaya Al-Maadeed, Ahmed Bouridane, ‘‘Image Steganography: A Review of the Recent Advances’’ VOLUME 9, February 10, 2021

[11] Y. Huang, C. Chang and C. Wu, “A DNA-based data hiding technique with low modification rates”, Multimedia Tools and applications. Vol. 70, No. 3, pp. 1439-1451, 2014.

[12] Yunpeng Zhang, Bochen Fu, and Xianwei Zhang, "DNA cryptography based on DNA Fragment assembly," In Information Science and Digital Content Technology (ICIDT), IEEE International Conference on, vol. 1, pp. 179-182, (2012)

[13] Srilatha, N., & Murali, G. (2016). Fast three level DNA Cryptographic technique to provide better security. 2016 2nd International Conference on Applied and Theoretical Computing and Communication Technology (iCATccT). doi:10.1109/icatcct.2016.7912037

[14] Akiwate, B., & Parthiban, L. (2018). A Dynamic DNA for Keybased Cryptography. 2018 International Conference on Computational Techniques, Electronics and Mechanical Systems (CTEMS). doi:10.1109/ctems.2018.8769267