IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, November 2022
Impact Factor: 6.252

Hybrid Encryption Model using One-Time Pad and Route Cipher algorithm with Integrity Check (Using MD5 hashing)

Niyanth Guruprasad, Sushanth Ravishankar, Dr. R. Renuka Devi
Department of Computing Technologies
SRM Institute of Science and Technology, Chennai, India
niyanthgp@gmail.com, sushanthpvr@gmail.com, renukadr@srmist.edu.in

Abstract: *The world is moving forward in terms of internet connectivity. While this enhances connectivity and strengthens communication, it brings with it its shortcomings. The advent of internet went hand in hand with emergence of hackers. This made businesses vulnerable and prone to malicious attacks by various groups and organizations. The business, to safeguard the data of the clients and consumers had to fool proof their servers and data-centres, hence the need to enhance and tighten security and close various vulnerable points. Cryptography is a technique involving encryption of data and messages so that only the intended audience can decrypt and comprehend it. For enhanced security, a hybrid encryption technique along with integrity check (MD5 hashing) is used. The encryption technique of One Time Pad (OTP - symmetric) and Route cipher (trans- positional) are combined and used.*

Keywords: Hybrid Encryption, Symmetric and Asymmetric Cryptography Algorithm, Encryption and Decryption, Message- Digest5, One-Time Pad Cipher

I. INTRODUCTION

The majority of people now rely mostly on the internet to send data from one end of the earth to the other due to technical breakthroughs that have brought about the current status of the world. Messages, chats, and other formats are just a few of the ways that data can be delivered over the internet. The data alteration can be carried out online very quickly, precisely, and quickly. Anyhow, one of the main concerns with sending data over the internet is the ”security risk” it poses; for instance, personal or confidential information can be hidden or compromised from a variety of angles [1] . In this way, considering data security becomes necessary because it is one of the most important factors to take into account when transferring data.

Cryptographic algorithms both symmetric and asymmetric have benefits and drawbacks. Asymmetric algorithms offer more capability than symmetric ones, but at the trade-off of slower performance and more expensive hardware. Symmetric encryption, on the other hand, offers effective and affordable ways to secure data without sacrificing security and ought to be thought of as the best and most suitable security solution for many applications. The complimentary use of symmetric and asymmetric encryption may be the best option in some circumstances. By avoiding their drawbacks, hybrid encryption aims to take advantage of both algorithm classes’ advantages [2].

1.1 Symmetric Cryptography

A secret key and an encryption algorithm are used in sym- metric encryption to convert plain-text into cipher-text. The cipher-text is decrypted using the same key and a decryption technique to reveal the plain-text. The author noted the lengthy history of symmetric-key encryption. The different symmetric key cryptography algorithms include, but are not limited to (AES, DES, and Blow-fish) [2] [7].

1.2 Asymmetric Cryptography

Data is encrypted and decrypted using several keys when using asymmetric key encryption, commonly known as public key cryptography. Each participant in this system has two keys: a public key that is known by everyone and is kept secret, whilst the private key is shared with only the intended receiver. Even though they appear to be different, the public

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, November 2022
Impact Factor: 6.252

and private keys are mathematically related. There is a corresponding private key for every public key. This approach may provide nonrepudiation, authentication, and integrity [2] [7].

1.3 Hashing

Another approach to secure the data from being tampered or accessed by threat actors can be done using hashing. The hash function is used in the hashing algorithm, which specifies how the message will be divided up and how the results from earlier message blocks will be linked together. A message or piece of data is hashed to produce a singular signature with a specified length. It is frequently used to verify the accuracy of data.

A popular cryptographic hash function that generates a 128-bit (16-byte) hash value is the Message-digest (MD5) algorithm [3]. It has been applied in many different security-related applications.

II. SECURITY CHALLENGES PRESENT IN INFORMATION SYSTEMS

Information systems encompasses all the components that play a role in collecting, storing, processing data for providing information to businesses. Information security, or infosec as it is frequently referred to, is a collection of procedures designed to protect data from unauthorized access or modification both during storage and transmission from one system to another [5]. It may also occasionally be referred to as data security. Abbreviated as the CIA—confidentiality, integrity, and availability—best sums up the fundamental elements of information security.

- Confidentiality - Techniques to guarantee confidentiality include passwords, encryption, authentication, and security against penetration assaults.
- Integrity - refers to keeping data accurate and guarding against improper modification, whether unintentionally or on purpose.
- Availability - A solid backup strategy must be put in place for disaster recovery, and network and computing resources must be matched to the level of data access you anticipate.

2.1 Information System Problems

Threats to information security can take many different forms, including software attacks, intellectual property theft, identity theft, equipment theft, information theft, sabotage, and information extortion.

- Threats can be anything that can exploit a weakness in security to hurt, destroy, or negatively affect an object or objects of interest.
- Attacks from software include those caused by viruses, worms, Trojan horses, etc. A lot of consumers think that malware, viruses, worms, and bots are all the same thing. The only thing they have in common, however, is that they are all malicious programs, each of which behaves in a distinct way.
- Malware is an acronym for malicious software and malicious software. Malware, then, is essentially anything that is intended to do harm, whether it be intrusive program code or malicious software.

The above mentioned threats could be harmful and dangerous. They can lead to problems like:

- **Intellectual property** theft is the infringement of such rights as copyrights, patents, etc.
- **Identity theft** is the act of using another person's login information to gain access to someone else's personal information or critical information, such as gaining access to a person's computer or social media account.
- **Sabotage** refers to ruining a company's website in order to undermine client confidence.
- **Information extortion** is the theft of a company's assets or information with the intention of receiving cash. As an illustration, ransomware might lock victims' files, rendering them inaccessible, and demand payment in exchange. the victim's only after payment

2.2 Cryptography Problems

The usage of the same key for both encryption and decryp- tion is one of the greatest problems we encounter in symmetric cryptography. Since symmetric cryptography only uses one key, the loss or theft of the key will have a significant effect on security of data being stored in our systems

The creator of cryptographic algorithms like symmetric cryptography must research the tool and watch out for flaws before implementing it. For instance, some ciphers feature a set of "weak" keys, which are key values that make it

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, November 2022
Impact Factor: 6.252

simpler for a cunning adversary to crack. A security designer also encounters difficulties when implementing security solutions, such as random number generation, key management, certifi- cate revocation problems, trust models and so on.

III. LITERATURE SURVEY

[1] explains how to safeguard data from unauthorised access using the Vigenere cypher and Polybius Square cypher algorithms. The procedure of encrypting and decrypting data using the provided techniques is well explained in the article. Finally, with the use of flowcharts, it provides a methodology for how encryption and decryption on any data utilising the aforementioned algorithms function.

In [2], the design of a hybrid cryptography paradigm em- ploying symmetric and asymmetric cryptographic algorithms is discussed by the authors. The notion of symmetric and asymmetric algorithms, as well as their benefits and draw-backs, are explained in detail in the paper. It describes the hybrid model's architecture, which combines Binary RSA and substitution cypher. The report finally provides some insight into the advantages of employing a hybrid approach.

Paper [3]discusses the application of a similar hybrid cryp- tography approach to wireless sensor networks (WSN). The paper then briefly discusses the security issues with WSN. The method of the suggested hybrid cryptography protocol is then discussed in the study. By implementing the protocol in a sample simulation and tracking the outcomes in terms of ciphertext size, throughput, and processing time, it also evaluates the approach's robustness (for both encryption and decryption).

[3] gives us a revolutionary method for a cloud security system by combining the Blowfish and MD5 algorithms into a hybrid cryptography paradigm. The document goes into great depth regarding the techniques utilised, including the encryption and decryption procedures. Additionally, it provides a comparison of the RSA MD5 model with the aforementioned hybrid model in terms of file size, encryption, and decryption times.

The [5] author talks of the potential vulnerabilities in a cloud system and tries to resolve them an algorithm is proposed which will plug some of the vulnerabilities in the cloud system, with the algorithm being the combination of ECDSA, SHA256 and AES.

In [6] the author proposes a simple yet effective protocol with enhanced security involving ECC scheme and blind factor. The author has also proceeded to use techniques such as Elliptical Curve Cryptography and Dual RSA.

[7] The author talks of the talks data breaches and security issues in a cloud, by reviewing the past papers to enable the novice and the inexperienced ones to garner information regarding the same. The author talks of the shortcomings in research and attempts to overcome the same.

The author talks of various types of Polybius Square in cryptography. The author compares and contrasts various reference papers and their modified algorithms and codified the results obtained.

IV. METHODOLOGY

This paper proposes a novel cryptographic algorithm blend- ing two encryption schemes, namely the **One-Time pad cipher** and the **Route cipher**. The proposed model is much more secure and defeats all the shortcomings from previously proposed models [1]. Additionally the model also uses hashing methods for checking the integrity of data that has been sent over the network. The hashing algorithm that has been used is **MD5 hashing algorithm**.

4.1 One-Time Pad Cipher

In a one-time pad cipher, a message is encrypted using a randomly generated secret key just once, and the recipient decrypts it using the same key. The benefit of using randomness-based keys for message encryption is that there is theoretically no way to crack the code by looking at a series of messages. Important point to note is that the length of the secret key generated will be as long as the length of the plain-text message to be encrypted itself.

Encryption:

1. Input the plain-text, X
2. The secret key is generated and is as long as the message plaintext itself,K
3. FOR itr =0 to len(plain-text):
4. cipher-text = X[i] XOR K[i]
5. We have the cipher text ready

Decryption

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, November 2022
Impact Factor: 6.252

4.2 Route Cipher

The route cipher belongs to a type of cipher class known as transposition cipher. This works by having letters of a text arranged in a grid and be read along a predetermined course or route, like a serpentine road. The path most commonly starts from the top right corner of the grid. Following the specified path, the plaintext is read off after being written in a grid. It rearranges the plaintext characters according to the contour of a fictitious path shown on a grid.

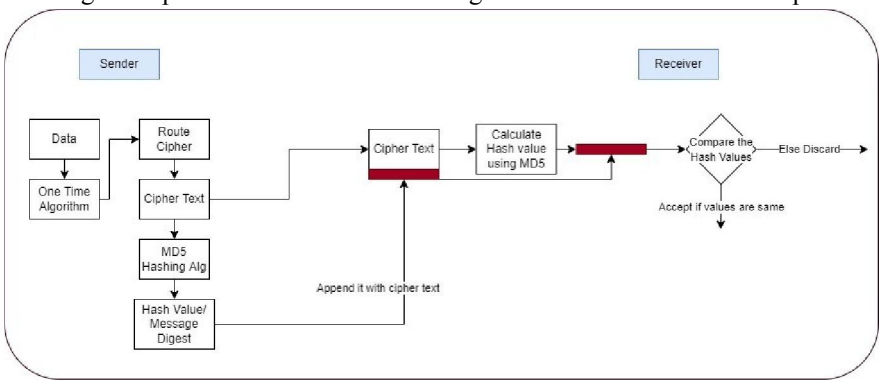

Figure 1: Flowchart of the Hybrid Encryption Model

Encryption:

1. Get the input, P
2. Select a matrix table of 4 rows and x columns.
3. X because you need to fit all char's of P in the matrix.
4. Start arranging the char's in the matrix from left-right
5. Pad empty spaces with a null character like x or 0
6. Start at top right corner of matrix and go in clockwise direction
7. Track the letters and you will have the cipher text

Decryption

1. Start assembling the char's from top right corner in clockwise direction
2. Once completed remove all padding char's
3. Now get plain text by reading matrix left-right rowise

4.3 MD5 Algorithm

The MD5 (message-digest algorithm) cryptographic tech- nique is used for digital signatures, content verification, and message authentication [4]. Based on a hash algorithm, MD5 checks that a file you send and the recipient both receive the same file. To create a signature that can be compared to the original file, MD5 processes whole files using a mathematical hashing method [6]. In this manner, it will be possible to verify that a file received matches the one that was transmitted, guar- anteeing that the correct files are delivered to their intended locations.

So the model as mentioned before uses a combination of one-time pad cipher and route cipher algorithms to encrypt

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, November 2022
Impact Factor: 6.252

data. The first stage in encryption begins with the one-time pad cipher. A random secret key is generated which then starts the process of encryption. By the end of the first stage we get the first layer of encrypted data.
The second layer starts by encrypting this cipher-text further using route cipher algorithm. Towards the end of encryption stage we will have a cipher-text that is relatively harder to crack utilizing crypt-analysis methods.

V. CONCLUSION

Encryption is the art of keeping information secure by transforming it into a form unintelligible to unintended re-cipients. Involving simple and weak cipher would ensure the message has been tampered with. So our work proposes and implements a hybrid cryptographic model. The new system seeks to increase computing speed and present a better hybrid system while taking into consideration the current issues and flaws of various models. For enhanced protection, we've paired a symmetric cypher called One Time Pad with the route cypher and an integrity check using the MD5 hashing technique. As a result, a strong system is created that is challenging for attackers to breach. Overall, this leads to a model improvement with faster encryption and decryption processes and increased security.

REFERENCES

[1]. S. Vatshayan, R. A. Haidri and J. Kumar Verma, "Design of Hybrid Cryptography System based on Vigene`re Cipher and Polybius Cipher," 2020 International Conference on Computa- tional Performance Evaluation (ComPE), 2020, pp. 848-852, doi: 10.1109/ComPE49325.2020.9199997.

[2]. Chaudhari, Swapnil. (2018). A Research Paper on New Hybrid Cryp- tography Algorithm.

[3]. Y. Alkady, M. I. Habib and R. Y. Rizk, "A new security protocol using hybrid cryptography algorithms," 2013 9th International Com- puter Engineering Conference (ICENCO), 2013, pp. 109-115, doi: 10.1109/ICENCO.2013.6736485.

[4]. A. Chauhan and J. Gupta, "A novel technique of cloud security based on hybrid encryption by Blowfish and MD5," 2017 4th International Conference on Signal Processing, Computing and Control (ISPCC), 2017, pp. 349-355, doi: 10.1109/ISPCC.2017.8269702.

[5]. V. K. Soman and V. Natarajan, "An enhanced hybrid data security algorithm for cloud," 2017 International Conference on Networks and Advances in Computational Technologies (NetACT), 2017, pp. 416-419, doi: 10.1109/NETACT.2017.8076807.

[6]. M. J. Dubai, T. R. Mahesh and P. A. Ghosh, "Design of new security algorithm: Using hybrid Cryptography architecture," 2011 3rd Interna- tional Conference on Electronics Computer Technology, 2011, pp. 99- 101, doi: 10.1109/ICECTECH.2011.5941965.

[7]. S. A. Ahmad and A. B. Garko, "Hybrid Cryptography Algorithms in Cloud Computing: A Review," 2019 15th International Conference on Electronics, Computer and Computation (ICECCO), 2019, pp. 1-6, doi: 10.1109/ICECCO48375.2019.9043254.

[8]. Arroyo, Jan Carlo and Dumdumaya, Cristina and Delima, Allemar Jhone. (2020). Polybius Square in Cryptography: A Brief Review of Literature. International Journal of Advanced Trends in Computer Sci- ence and Engineering. 9. 3798-3808. 10.30534/ijatcse/2020/198932020.

[9]. X. Li, L. Yu and L. Wei, "The application of hybrid encryption algorithm in software security," 2013 3rd International Conference on Consumer Electronics, Communications and Networks, 2013, pp. 669-672, doi: 10.1109/CECNet.2013.6703419.

[10]. Q. Zhang, "An Overview and Analysis of Hybrid Encryption: The Combination of Symmetric Encryption and Asymmetric Encryption," 2021 2nd International Conference on Computing and Data Science (CDS), 2021, pp. 616-622, doi: 10.1109/CDS52072.2021.00111.

[11]. G. P. Kanna and V. Vasudevan, "Enhancing the security of user data using the keyword encryption and hybrid cryptographic algorithm in cloud," 2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT), 2016, pp. 3688-3693, doi: 10.1109/ICEEOT.2016.7755398.

[12]. D. S. Solanki and S. Shiwani, "A model to secure e-commerce transac- tion using hybrid encryption," 2014 International Conference on Con- trol, Instrumentation, Communication and Computational Technologies (ICCICCT), 2014, pp. 642-645, doi: 10.1109/ICCICCT.2014.6993040.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, November 2022
Impact Factor: 6.252

[13]. Y. S. Gunjal, M. S. Gunjal and A. R. Tambe, "Hybrid Attribute Based Encryption and Customizable Authorization in Cloud Com- puting," 2018 International Conference On Advances in Communica- tion and Computing Technology (ICACCT), 2018, pp. 187-190, doi: 10.1109/ICACCT.2018.8529627.

[14]. Saravanan, P., Kumar, R.H., Arvind, T., Narayanan, B. (2019). Hybrid Cryptosystem Using Homomorphic Encryption and Elliptic Curve Cryp- tography Algorithm, i-manager's Journal on Computer Science, 7(1), 36-42. https://doi.org/10.26634/jcom.7.1.15667

[15]. Goyal, Kashish and Supriya Kinger. "Hybrid Approach Using Encryption Algorithms For Data Storage." (2013).