International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 7, Issue 5, pp 351-356, May-2023

https://doi.org/10.47001/IRJIET/2023.705052

Secure Cloud Storage Using Hybrid Cryptography

[1]Shruti Kambali, [2]Ghanshyam Gadekar, [3]Poorva Padave, [4]Poorva Patil, [5]Prof. Swati Vyas

[1,2,3,4]Student, Smt. Indira Gandhi College of Engineering, Ghansoli, New Mumbai, Maharashtra, India

[5]Professor, Dept. of AI & ML, Smt. Indira Gandhi College of Engineering, Ghansoli, New Mumbai, Maharashtra, India

***Abstract* - This proposed hybrid algorithm can be made much more powerful and secure by increasing the number of iterations in the encryption algorithm to suit the level of security required. An inverse policy of reducing the number of iterations for lower security can also be employed. Blowfish used for the encryption of file slices takes minimum time and has maximum throughput for encryption and decryption from other symmetric algorithms. The idea of splitting and merging adds on to meet the principle of data security. This system can be implemented into banking and corporate sectors to securely transfer confidential data in the world of data being the key asset, safeguarding our asset are primary responsibility. Communications, databases, infrastructure, transactions, knowledge; an organization's data is arguably its most valuable asset. It is in a business' best interests to keep its information safe, regardless of legal or regulatory requirements. For data security and privacy protection issues, the fundamental challenge of separation of sensitive data and access control is fulfilled. Cryptography technique translates original data into unreadable form. Cryptography technique is divided into symmetric key cryptography and public key cryptography. This technique uses keys for translate data into unreadable form. So only authorized person can access data from cloud server. Cipher text data is visible for all people.**

Keywords: AES, Advanced Encryption, Standard, DES, Data Encryption Standard, IDEA, International Data Encryption Algorithm, RC6, Rivest cipher 6, ECC, Elliptic Curve Cryptography.

I. INTRODUCTION

Internet is a public-interacted system; the amount of information exchanged over the Internet is completely not safe. Protecting the information transmitted over the network is a difficult task and the data security issues become increasingly important. In recent years, a Controversy has arisen over so-called strong encryption.

This refers to ciphers that are essentially unbreakable without the decryption keys. While most companies and their Customers view it as a means of keeping secrets and minimizing fraud, some governments View strong encryption as a potential vehicle by which terrorists might evade authorities. These governments, including that of the United States, want to set up a key-escrow Arrangement. This means everyone who uses a cipher would be required to provide the Government with a copy of the key. Decryption keys would be stored in a supposedly secure Place, used only by authorities, and used only if backed up by a court order. Opponents of This scheme argue that criminals could hack into the key-escrow database and illegally obtain, steal, or alter the keys. Supporters claim that while this is a possibility, implementing the key escrow scheme would be better than doing nothing to prevent Criminals from freely using encryption/decryption. At present, various types of Cryptographic algorithms provide high security to information on networks, but they are also having some drawbacks. To improve the strength of these algorithms, we propose a new hybrid cryptographic algorithm in this paper. The algorithm is designed using combination of two symmetric cryptographic techniques. These two primitives can be achieved with the Help of Data Encryption Standard (DES) and International Data Encryption Standard (IDEA). This new hybrid cryptographic algorithm has been designed for better security with integrity.

Cloud storage also helps in immediate data exchange, thus giving access to multiple people. This makes this service a perfect tool for both distant and in-house work. Thus, online cloud storage and is beneficial for all types of businesses. Cloud storage is a more cost-efficient platform that does not require a huge investment and it can be actively used for connecting and collaborating with clients and employees. Hence more and more users are turning to cloud storage, making it a very popular alternative to traditional storage options.

1.1 Research Paper Analysis

Hybrid Cryptography concept is used for securing storage system of cloud. Two different approaches are used to show the difference between less secure and more secure systems. The first approach uses RSA and AES algorithms; RSA is used for key encryption and AES is used for text or data encryption. In the second or we can say more secured approach, AES and Blowfish algorithms are used. In this approach, these two Algorithms provide double encryption over data and key which provides high security compared to the first one.

International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 7, Issue 5, pp 351-356, May-2023

https://doi.org/10.47001/IRJIET/2023.705052

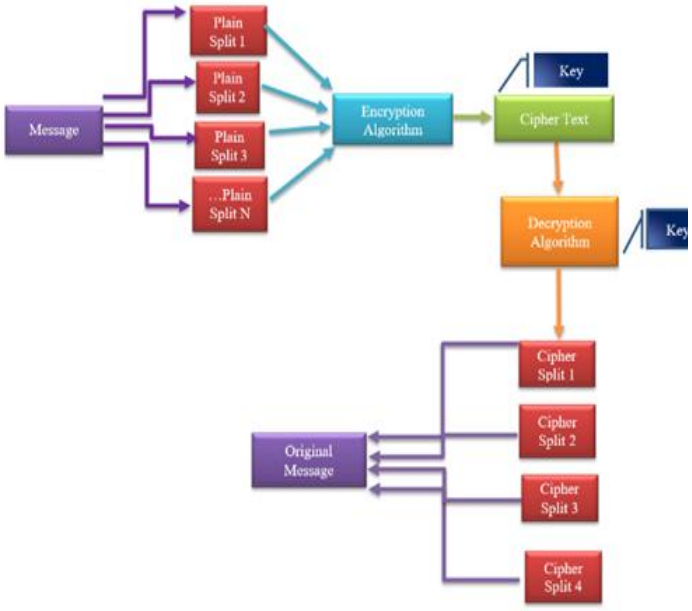


Figure 1: System Architecture

To make the centralized cloud storage secure ECC (Elliptic Curve Cryptography) algorithm is implemented. This approach uses single key for encryption and decryption and complete process takes place at the client side. This methodology performs steps such as:

a) Authentication
b) Key generation operation
c) Encryption
d) Decryption

II. METHODOLOGY

In the world of data being the key asset, safeguarding our asset is primary responsibility. Communications, databases, infrastructure, transactions, knowledge; an organization's data is arguably its most valuable asset. It is in a business' best interests to keep its information safe, regardless of legal or regulatory requirements. A system which stores data after encryption. This prevents data leak if a breach occurred. Any form of data can be stored. It ensures data confidentiality to users. This proposed hybrid algorithm can be made much more powerful and secure by increasing the number of iterations in the encryption algorithm to suit the level of security required. An inverse policy of reducing the number of iterations for lower security can also be employed. We can also go for combining another algorithm that will encrypt data given by the IDEA algorithm.

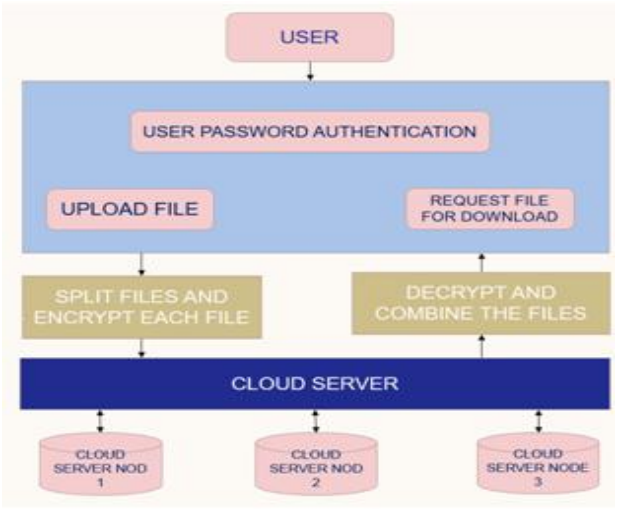
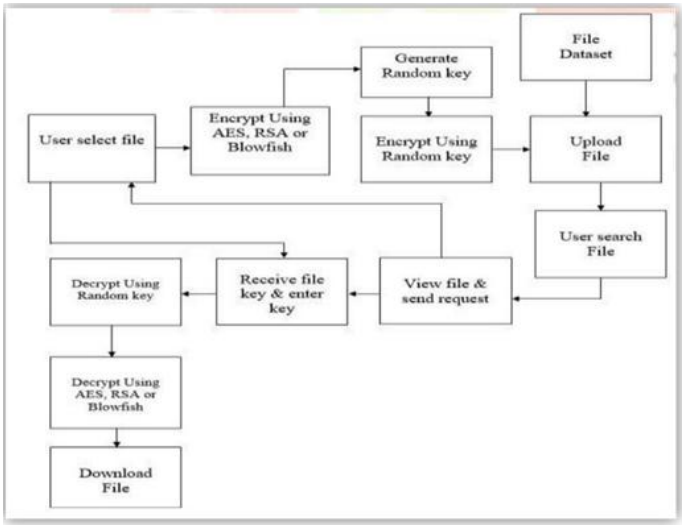


Figure 2: Sequence Diagram

2.1 Steps for Hybrid Cryptography algorithm



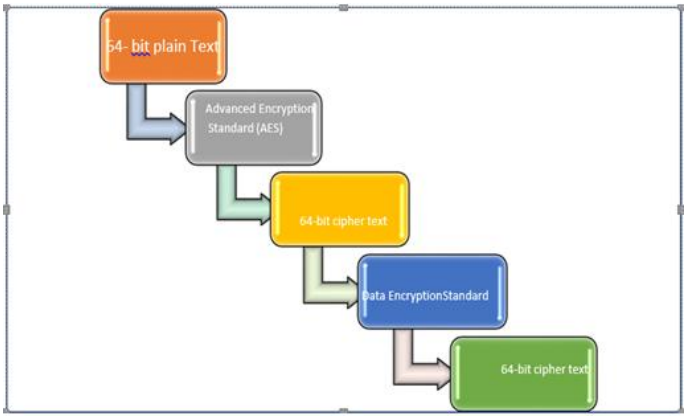


Figure 3: Sequence Diagram

DES takes an input of 64-bit plaintext data block and 56-bit key (with 8 bits of parity) and Outputs a 64-bit cipher text block.

International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 7, Issue 5, pp 351-356, May-2023

https://doi.org/10.47001/IRJIET/2023.705052

i. The 8 parity bits are removed from the key by subjecting the key to its Key Permutation.
ii. The plaintext and key are processed in 16 rounds consisting.
iii. The key is split into two 28-bit halves.
iv. Each half of the key is shifted (rotated) by one or two bits, depending on the round. The halves are recombined and subject to a Compression Permutation to reduce the key from 56 bits to 48 bits. This Compressed Key is used to encrypt this round's plaintext block.
v. The rotated key halves from step 2 are used in next round.
vi. The data block is split into two 32-bit halves.
vii. One half is subject to an Expansion Permutation to increase its size to 48 bits.
viii. Output of step 6 is exclusive-OR'ed with the 48-bit compressed key from step 3.
ix. Output of step 7 is fed into an S-box, which substitutes key bits and reduces the 48-bit.
x. Block back down to 32-bits.
xi. Output of step 8 is subject to a P-box to permute (scramble) the bits.
xii. The output from the P-box is exclusive-OR'ed with the other half of the data block.
xiii. After 16 rounds, the resultant is cipher text.This resultant cipher text is a input for the IDEA.

The 52 16-bit key sub-blocks which are generated from the 128-bit key are produced As follows:

First, the 128-bit key is partitioned into eight 16-bit sub-blocks which are then directly Used as the first eight key sub-blocks. The 128-bit key is then cyclically shifted to the left by 25 positions, after which the Resulting128-bit block is again partitioned into eight 16-bit sub-blocks to be directly used as the next eight key sub-blocks.

The cyclic shift procedure described above is repeated until all of the required 52 16-bit Key sub-blocks have been generated.

2.3 Workflow of System

The system is designed such that it works in the following way:

- The user then selects the file that is to be uploaded by browsing from local storage.
- The user then selects the encryption algorithm that they want to use. The proposed system provides the choice between using a combination of AES and RSA or AES and Blowfish.
- The selected file gets uploaded after getting encrypted using the selected encryption algorithm combination.
- The user also has the option of viewing the files that they have uploaded or have access to and downloading them.

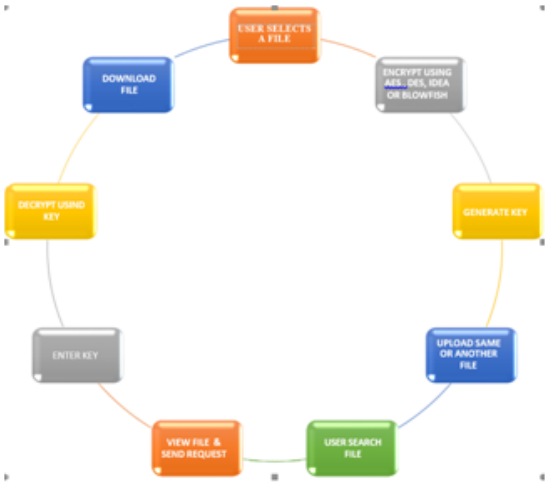


Figure 4: Workflow of System

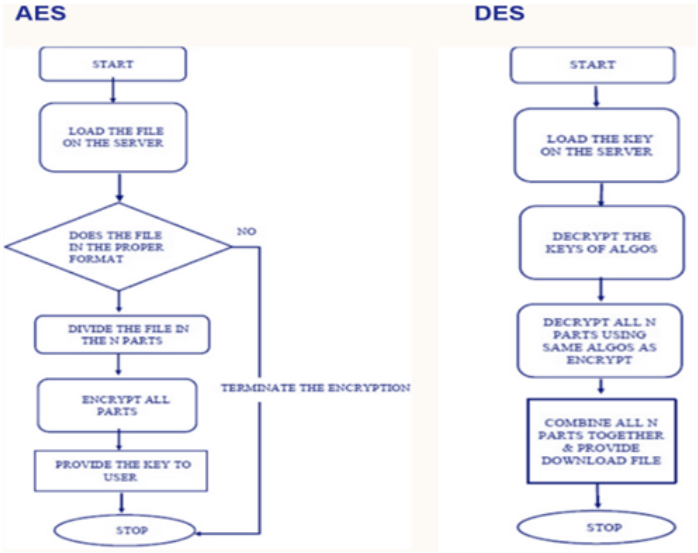
2.4 System Implementation

AES Algorithm:

The Advanced Encryption Standard (AES) also known as 'Rijndael' is a symmetric-key block cipher algorithm having three fixed 128-bit block ciphers with cryptographic key sizes of 128, 192 and 256 bits respectively.

The AES algorithm has maximum block size of 256 bits whereas Key size is unlimited. The AES design is based on a substitution-permutation network (SPN) and does not use the Data Encryption Standard (DES) Feistel network, thus making it stronger and faster than Triple-DES.

Step-wise description of the algorithm:



International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

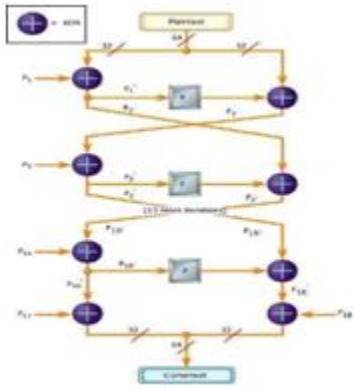
Volume 7, Issue 5, pp 351-356, May-2023

https://doi.org/10.47001/IRJIET/2023.705052

Key-expansion:

It will convert a key into several sub key arrays totaling 4168 bytes consisting at most 448 bits. Blowfish uses five subkey-arrays:

One 18-entry P-array consisting of 32-bit sub keys:



P1,P2,.,P18 and four 256-entry S-boxes of 32-biteach:

S1,0, S1,1,. S1,255
S2,0, S2,1,. S2,255
S3,0, S3,1,. S3,255
S4,0, S4,1,. S4,255

These keys are generated earlier to any data encryption or decryption.

DES Algorithm:

Data Encryption Standard (DES) is a symmetric-key block cipher.
Encrypts data in blocks of size of 64 bits each and Key length is 56 bits.
DES is based on the two attributes: substitution and transposition.
DES consists of 16 rounds. The result of this process produces 64-bit cipher text.

III. RESULTS AND DISCUSSIONS

3.1 Key Management:

The security of cryptographic systems relies on the secure storage and distribution of keys used for encryption and decryption. Key management can be a complex issue, especially for large-scale systems or when multiple parties are involved. Key distribution and key revocation are also significant challenges that must be addressed.

3.2 Performance:

Cryptographic algorithms, especially those used for public key cryptography, can be computationally intensive and may slow down the storage and retrieval of files. This can be a particular issue when dealing with large files or high volumes of data.

3.3 Complexity:

Cryptographic systems can be complex and require specialized knowledge to implement and manage. This complexity can lead to errors, vulnerabilities, and mistakes that can compromise the security of the system.

3.4 Compatibility:

Different cryptographic systems may not be compatible with each other, making it challenging to share files securely between different systems or platforms.

3.5 Attack and Security:

Cryptographic systems can be vulnerable to various types of attacks, including brute force attacks, side-channel attacks, and cryptographic attacks, such as birthday attacks and chosen plaintext attacks. Additionally, the security of cryptographic systems can be compromised by key management issues, implementation errors, and other vulnerabilities securely.

Objectives:

i. To eliminates the need for carrying physical storage devices.
ii. To provide Cloud storage safe backup, as opposed to physical storage devices where loss of device data.
iii. Corruption by a computer virus, natural disasters, amongst other causes, can lead to loss of data.
iv. To make the storage more cost-effective & to eliminate the need to invest in hardware.
v. To make storage help developers collaborate and share their work in a more efficient and speedy Manner.

International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

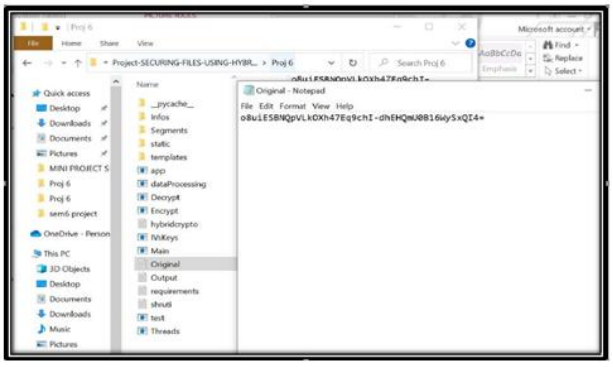
Volume 7, Issue 5, pp 351-356, May-2023

https://doi.org/10.47001/IRJIET/2023.705052

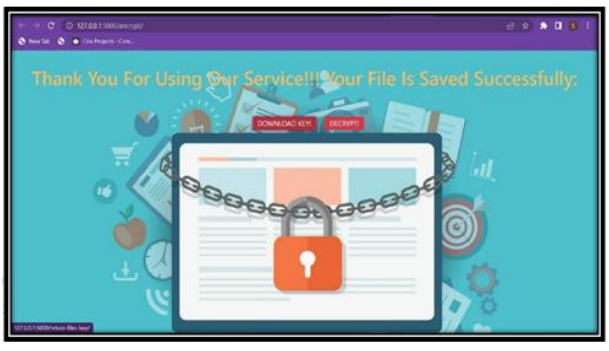
File Encryption Page:

File to Encrypt:

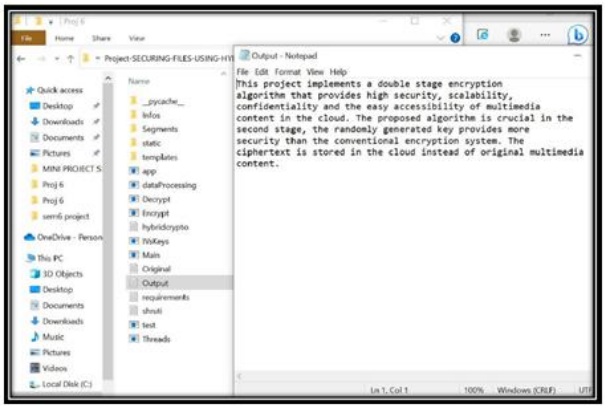
Once File gets Encrypted:



To Decrypt File:

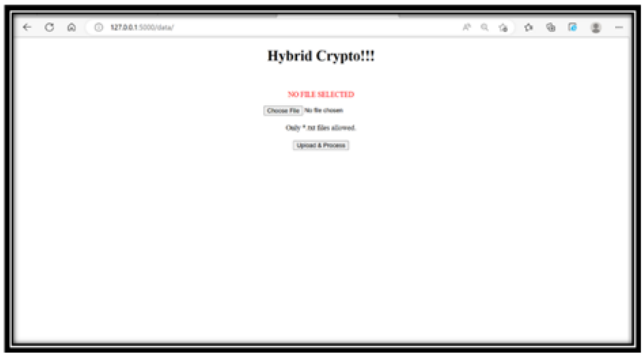


Decrypted File: We got original final i.e. (deciphered file)



Once File gets Decrypted:

If No File Chosen:



IV. CONCLUSION

This project implements a double stage encryption algorithm that provides high security, scalability, confidentiality and the easy accessibility of multimedia content in the cloud. The proposed algorithm is crucial in the second stage, the randomly generated key provides more security than the conventional encryption system. The cipher text is stored in the cloud instead of original multimedia content. Thus, the multimedia content is safe in the cloud.

ISSN (online): 2581-3048
Volume 7, Issue 5, pp 351-356, May-2023
https://doi.org/10.47001/IRJIET/2023.705052

V. FUTURE SCOPE

In the world of data being the key asset, safeguarding our asset is primary responsibility.

Communications, databases, infrastructure, transactions, knowledge; an organization's data is arguably its most valuable asset. It is in a business' best interests to keep its information safe, regardless of legal or regulatory requirements.

- A system which stores data after encryption.
- This prevents data leak if a breach occurred.
- Any form of data can be stored.
- It ensures data confidentiality to users.

ACKNOWLEDGEMENT

As every project is ever complete with the guidance of experts. So we would like to take this opportunity to thank all those individuals who have contributed in visualizing this project.

We express our deepest gratitude to our project guide Prof Swati Vyas (CSE (AIML)) Department, Smt. Indira Gandhi College of Engineering, University of Mumbai) for her valuable guidance, moral support and devotion bestowed on us throughout our work.

We would also take this opportunity to thank our project coordinator Prof. SWATI VYAS for her guidance in selecting this project and also for providing us all the details on proper presentation of this project.

We extend our sincere appreciation to our entire professors from Smt. Indira Gandhi College of Engineering for their valuable inside and tip during the designing the project. Their contributions have been valuable in many ways that we find it difficult to acknowledge them individually.

We are also grateful to our HOD Prof. SONALI DESHPANDE for extending his help directly and indirectly through various channels in our project.

If I can say in words I must at the outset my intimacy for receipt of affectionate care to Smt. Indira Gandhi College of Engineering for providing such a simulating atmosphere and wonderful work environment.

REFERENCES

[1] Sombir Singh, Sunil k. Maakar, Dr. Sudesh Kumar "Enhancing the Security of DES Algorithm Using Transposition Cryptography Techniques", IJARCSSE, Volume 3, Issue 6, pp 464-470, June 2013.
[2] Nick Hoffman "A Simplified IDEA Algorithm" Department of Mathematics, Northern Kentucky University pp 1-5, 2007.
[3] Meier, W., On the Security of the IDEA block cipher, Advances in Cryptology.
[4] Atul Kahate "Cryptography and Network Security" second edition.
[5] Shaaban Sahmoud, Wisam Elmasry and Shadi Abdulfa "Enhancement the security of AES againt modern attacks by using variable key block cipher".
[6] Data Encryption Standard (DES), Federal Information processing standards, Publication 46-3, 1999 October 25.
[7] Advanced Encryption Standard, National Institute of Standards and Technology (US).
[8] URL:http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf
[9] William Stallings:"Cryptography and network security: Principles and Practices".
[10] Advanced Encryption Standard, [online], Available URL: http://en.wikip/Advanced_Encryption_Standard
[11] T.S. Chen, H.-W. Tsai, Y.-H. Chang, and T.-C. Chen, "Geographic converge cast using mobile sink in wireless sensor networks," Comput. Commun., vol. 36, no. 4, pp. 445–458, Feb. 2013.
[12] Clustering and routing in wireless sensor networks," Comput. Netw., vol. 55, no. 13, pp. 2803–2820, Sep. 2011.
[13] William Stallings:"Cryptography and network security: Principles and Practices".

Citation of this Article:

Shruti Kambali, Ghanshyam Gadekar, Poorva Padave, Poorva Patil, Prof. Swati Vyas, "Secure Cloud Storage Using Hybrid Cryptography" Published in *International Research Journal of Innovations in Engineering and Technology - IRJIET*, Volume 7, Issue 5, pp 351-356, May 2023. https://doi.org/10.47001/IRJIET/2023.705052

****

