International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 11 Issue: 09 | Sep 2024 www.irjet.net p-ISSN: 2395-0072

ENCRYPTION AND DECRYPTION USING AES

[1]K.Venkateswarlu, [2]Sree Chithra Yellanki

Department of Computer Science and Systems Engineering, Andhra University College of Engineering, Andhra Pradesh, India[1]
Department of Computer Science and Systems Engineering, Andhra University College of Engineering, Andhra Pradesh, India[2]

Abstract

Cybercrime is more prevalent than ever all over the world. Consequently the ability to protect sensitive information is being crucial. Hacking and phising emails are seen these days and gives us a task to create a software that protects data. In this paper, we perform file encryption and decryption i.e., encryption is encoding files and decryption is decoding files that have sensitive data. This means that the attacker or malware with access to one's computer cannot read the sensitive data unless the attacker has the encryption- decryption key, even if attacker has encryption-decryption key and tries to access data the file content are stored in unreadable format.

"Encryption conceals data by scrambling it, so that anyone who tries to view it sees only random information. Encrypted data can only be unscrambled through the process of decryption."

***Key Words*: Encryption, Decryption, Advanced Encryption Algorithm, Malware, Hacker**

1.INTRODUCTION

By the advancement of web in today's world endless number of employees have increased that require sharing of records and folders. Security concerns with respects to information transmission and capacity are a major concern of both the transmitters and receivers. Cryptography is the fundamental stage in which present day data security, which includes the use of progressed scientific approaches in tackling difficult cryptographic issues, has gained its grounds within the computerized world. This gives the need of Encryption and Decryption utilizing AES.

1.1 ENCRYPTION AND DERCRPTION

Encryption, a crucial component of data security, plays a vital part in securing sensitive information within the computerized domain. It employs intricate numerical calculations to convert lucid data into garbled ciphertext, defending it from unauthorized access. Encryption give significance lies in its capacity to maintain privacy, judgment, and authenticity of data. It guarantees that data can be safe from unauthorized altering or debasement, and permits verification of the source and judgment of messages.

Also

- **File encryption:** This type of protection allows you to granularly protect individual files by encrypting them. This technique is excellent when you have specific files that need an extra degree of security or contain very sensitive information. Encrypting individual files gives you more control over access and assures that even if one file is hacked, the others will still be safe.

- **Folder encryption:** Encrypting whole folders and all the data included within them is a comprehensed approach. This solution might be helpful to safeguard a group of related files simultaneously. Encrypting folders simplifies the encryption procedure since you can protect several files simultaneously while retaining their structure and order.

Decryption is the method of changing information that has been rendered incoherent through encryption back to its decoded frame. In unscrambling, the framework extricates and changes over the confused information and changes it to effectively reasonable arrange.

A cryptographic key is a mathematical algorithm implemented in software or hardware and used to encrypt or decrypt data. It is a string of bits that are combined with the data to create cipher text. The cryptographic key can also be used to unencrypt data back to plaintext.

The two main types of cryptographic algorithms are symmetric and asymmetric. Symmetric key algorithms work by using a single key to encrypt and decrypt information, whereas asymmetric cryptography uses two keys:

A public key to encrypt messages and a private key to decode them.

i. In a Public key, two keys are utilized one key is utilized for encryption and another key is utilized for decryption. One key (public key) is utilized to scramble the plain content to convert it into cipher text and another key (private key) is utilized by the receiver to unscramble the cipher text to read the message.

ii. In Private key, the same key (secret key) is utilized for encryption and decryption. In this key is symmetric since the as it were key is copied or shared by another party to unscramble the cipher text. It is quick than public-key cryptography.

Here RSA can be used ,RSA encryption encompasses a number of distinctive errands that it is utilized for. One of these is computerized marking for code and certificates. Certificates can be utilized to verify who a public key has a place to, by signing it with the private key of the key pair owner. This verifies the key combine owner as a trusted source of data. Code marking is additionally done with the RSA calculation. To guarantee the owner is not sending dangerous or incorrect code to a buyer, the code is marked with the private key of the code creator. This verifies the code has not been altered maliciously in transit, which the code maker verifies that the code does what they have said it does.

Though practical in numerous circumstances, there are still a number of vulnerabilities in RSA that can be misused by attackers. One of these vulnerabilities is the execution of a long key within the encryption calculation. Algorithms like AES are unbreakable, whereas RSA depends on the measure of its key to be troublesome to break. The longer an RSA key, the more secure it is. Utilizing prime factorization, analysts overseen to break a 768 bit key RSA calculation, but it took them 2 years, thousands of man hours, and an foolish sum of computing control, so the currently utilized key lengths in RSA are still secure. The National Institute of Science and Technology (NIST) recommends a minimum key length of 2048 bits presently, but numerous organizations have been utilizing keys of length 4096 bits. Other ways RSA is vulnerable:

1.Weak Random Number Generator:

When organizations utilize weak arbitrary number generators, at that point the prime numbers made by them are much easier to calculate, in this way giving attackers an easier time of cracking the algorithm.

2.Weak key Generation

RSA keys have certain prerequisites relating to their generation. In case the prime numbers are too close, or if one of the numbers making up the private key is too small, at that point the key can be solved much easily.

3.Side channel Attacks

Side channel attacks are a strategy of attack that take advantage of the system running the encryption algorithm, as restricted to the algorithm itself. Attackers can analyze the control being utilized, use branch prediction analysis, or utilize timing attacks to find ways to discover the key utilized within the a, hence compromising the information. AES can overcome the issue given.

1.2 ADVANCED ENCRYPTION STANDARD(AES)

AES stands for Advanced Encryption Standard and is be a majorly utilized symmetric encryption algorithm. It is primarily utilized for encryption and security of electronic data. AES comprises of three block ciphers and these ciphers are used to supply encryption of information. It is a encryption calculation utilized to secure information by changing over it into an incoherent form with the right key. It is developed by the National Institute of Standards and Technology (NIST), AES encryption uses different key lengths (128, 192, or 256 bits) to supply strong security against unauthorized access. This information security degree is productive and broadly executed in securing web communication, ensuring sensitive information, and scrambling records. AES, a foundation of cuttingedge cryptography, is recognized globally for its capacity to keep data secure from cyber threats and all data that require web to operate.

2. PROPOSED METHODOLOGY

In previous paper, we have seen that the title of files and folders are scrambled and decoded for security reasons. The issue with is that on the off chance that the hacker gets to know the key one can study data show within the files and folders. This gives threat to the information security. Inorder to overcome this issue, I propose the following:

In this paper, we scramble and decode the names and content of the files and folders. Here the names of files and folders are saved with .aes extension . This helps to know that the file is encrypted. Now the encrypted files are stored in a encrypted folder. This allows a more prominent security to the files and folders, usually if the programmer gets to know the key used to scramble and unscramble the information, he cannot understand the information that's present because it is encrypted. Then a encryption key is given that can be used to decrypt the data. Typically the contents are in unscrambled form which cannot be understood. This gives more security to the information in such a way that it can be used by any organization.

If one wants to decrypt the data, one should enter the decryption key. Then one can have decrypted folder that has the files and folders that contain data that is decrypted into format.

In this, documents, folders that contain any data,pdf with any number of pages, images can be encrypted and decrypted using one key.

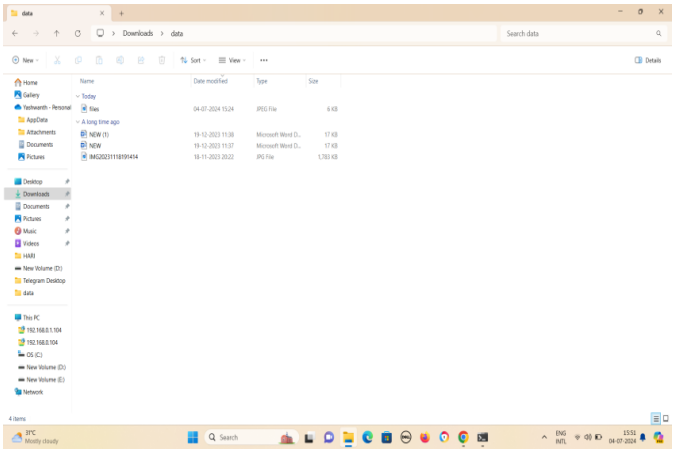

Fig-1: This is folder DATA that contains documents,images.

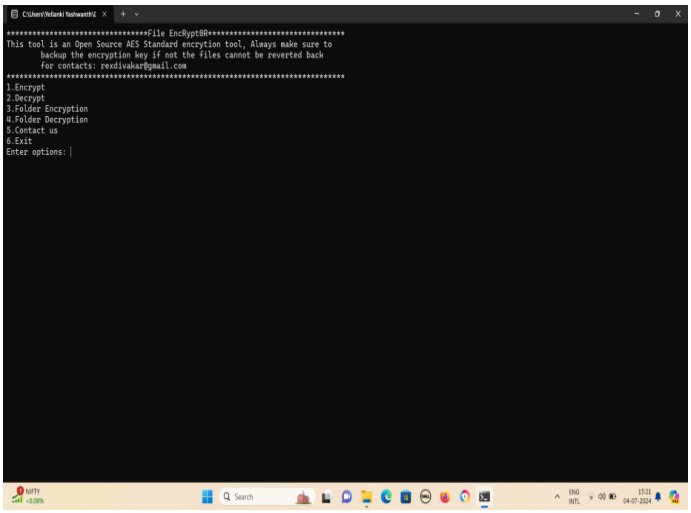

Fig-2: Options available: 1.Encrypt 2.Decrypt 3.Folder Encryption 4. Folder Decryption 5.Exit

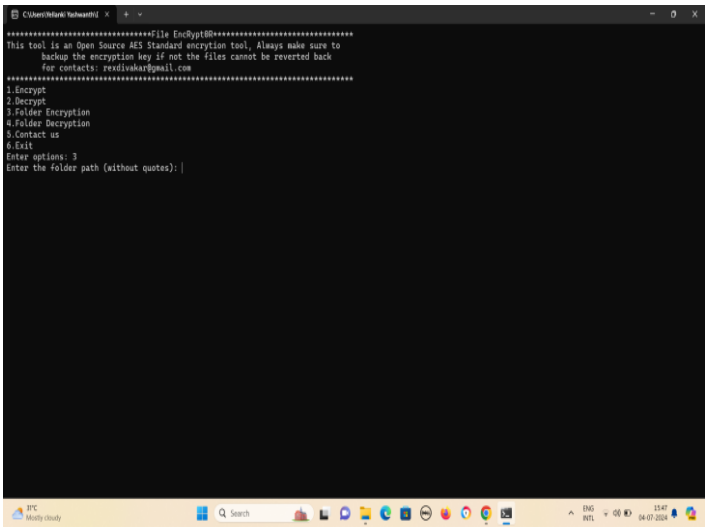

Fig-3: Select option 3 Folder Encryption

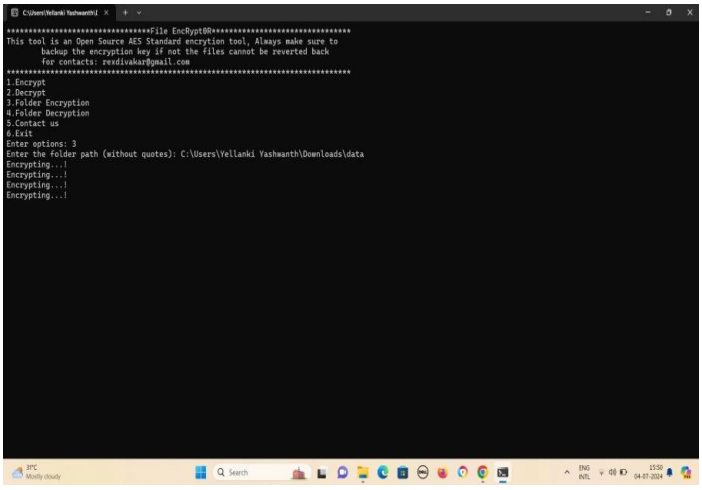

Fig-4: Screen showing Encryption is processed

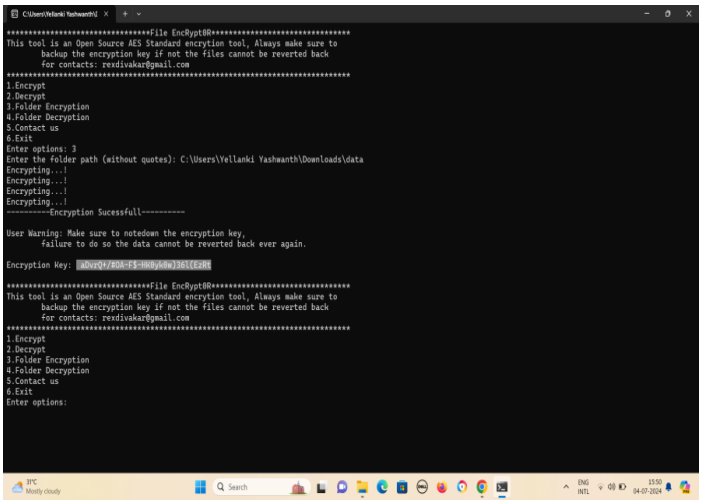

Fig-5: Folder is being encrypted and gives a encryption key that can be used for decryption

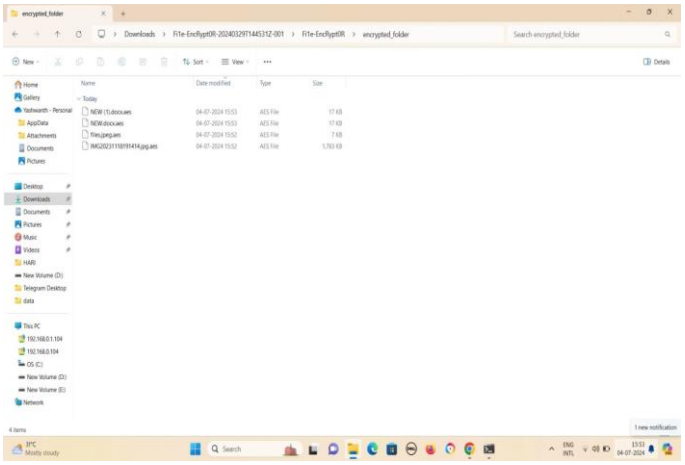

Fig-6: The encrypted folder is created where all documents, folders are encrypted (.aes).

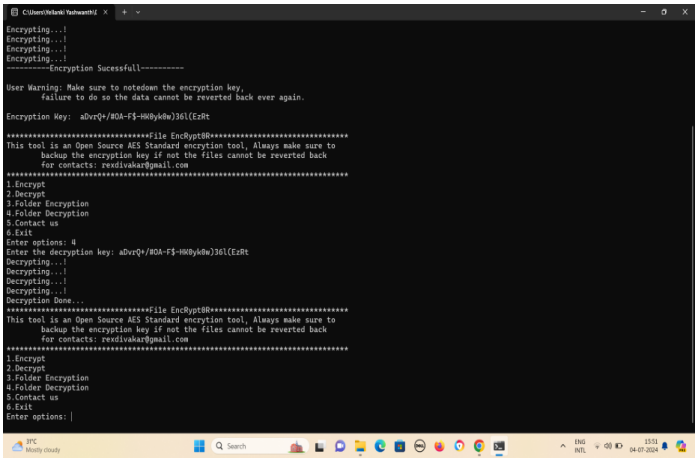

Fig-7: Select option 4 for Decryption and enter decryption key

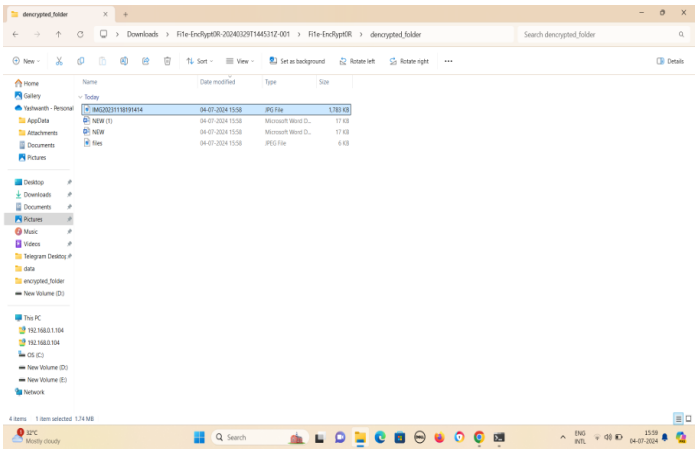

Fig 8: The decrypted folder is created

AES performs operations on bytes of data rather than in bits. Since the block size is 128 bits, the cipher processes 128 bits (or 16 bytes) of the input data at a time.

The number of rounds depends on the key length as follows :

Table -1: AES rounds:

128-bit key	10 rounds
192-bit key	12 rounds
256-bit key	14 rounds

Remark:

The below figure shows the encryption-decryption process using AES which includes operations

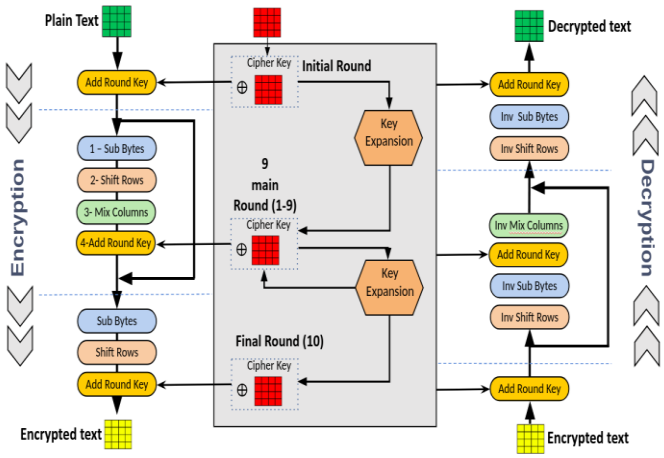

Fig -9: Encryption and Decrpytion process

3. CONCLUSIONS

In the recent years Encryption methods have made more secured frame of information transfer. From the perception of prior papers, we seem make the information security more complex by including more strategies to AES so that no programmers can extract the information easily. In this paper, strategies utilized in file encryption and decoding were talked about. The encryption methods such as AES is considered here. Consequently this paper makes a difference to send information in a more secure way compared to all the In essence, scrambling records gives a strong layer of security to defend critical data from prying eyes. We have previous study that only scrambles and decode the file or folder names. In this we are able see that names and contents of the file or folder can be scrambled.

ACKNOWLEDGEMENT:

Any algorithms like RSA can be used for this mechanism, according to my perspective AES is more secured to encrypt and decrypt data. This is because AES offers stronger security since it incorporates multiple rounds of encryption, making it harder to break, and harder for attackers to steal the encrypted information using brute-force attacks.

FUTURE SCOPE:

Encryption and Decryption using AES can be used in images. Convolutional Neural Network can be used to compress images more than by using AES. This allows to encrypt images with no loss[9].

REFERENCES

[1] Lu, D.: Computer Cryptography, Computer network data privacy and security. Tsinghua University Press (1998)

[2] Li, K., Wang, D., Dong, X.: Practical Cryptography and computer data security. Northeastern University Press (1997)

[3] Huang, Y., Chen, L., Tang, S.: Information security and encryption decryption core technology. Electronic Press (2001)

[4] Li, S., Wang, D.: Modern Cryptography Theory, Method and frontier. Science Press, Beijing (2009)

[5] Manzanares, A.I., Sierra, C.J.M., Marquez, J.T.: On the implementation of security policies with adaptative encryption. Computer Communications (2006)

[6] Bhargav, S., Majumdar, A., & Ramudit, S. (2008, Spring). 128-bit AES decryption. Retrieved November 21, 2020, from http://www.cs.columbia.edu/~sedwards/classes/2008/4840/reports/AES.pdf

[7] SPIEGEL. (2014, December 28). Inside the NSA's War on Internet Security - DER SPIEGEL - International. Retrieved November 21, 2020, from https://www.spiegel.de/international/germany/inside-the-nsa-s-war-on-internet-security-a-1010361.html

[8] [8] Thakkar, J. (2020, June 2). DES vs AES: Everything to Know About AES 256 and DES Encryption. Retrieved November 21, 2020, from https://sectigostore.com/blog/des-vs-aes-everything-to-know-about-aes-256-and-des-encryption/

[9] [9] Monkeypox detection and classification using multi-layer convolutional neural network from skin images https://www.arpnjournals.com/jeas/jeas_1123_9342.htm