A Novel Approach to Data Encryption - MADKEM

Hemang Mokariya
MSc Cyber Security and Cyber Law
Marwadi University – Rajkot
92100565003 mokariyahemang@gmail.com
Vaibhav Chhelavada
MSc Cyber Security and Cyber Law
Marwadi University – Rajkot
92100565002 vschhelavada07@gmail.com
Keshav Agrawal
MSc Cyber Security and Cyber Law
Marwadi University – Rajkot
92100565012 keshavagrawal4089@gmail.com
Dr.Ravirajsinh S. Vaghela,
MSc Cyber Security and Cyber Law Marwadi University - Rajkot
Ravirajsinh.vaghela@marwadieducation.edu.in

ABSTRACT

Data security comes as a priority for any organization around the globe. Be it user data or a company's internal confidential data, safety is a priority for it anywhere. Organizations use various encryption technologies to encrypt and secure the data this way. Different encryption technologies are widely used and proven to be secure. Yet, we can find some flaws we should cover to enhance data security. As computing speed and technologies such as gpu based reverse the hash which is now critical and required new answer against this gap. We are offering Madkem a secure and easy yet complex encryption technique which will efficiently allow adequate data security.

Keywords : **Cryptography, Encryption, Decryption, Security Key, Cryptology, AES, DES, PSA, Threefish, Two fish, 3DES, Blowfish**

INTRODUCTION

Internet Communication is a common thing nowadays. Transferring data and media over the internet is a piece of cake for us. With the data being transferred so commonly, the integrity of the media or message is also essential. To maintain the integrity of a message, encryption techniques were introduced. The roots of encryption go far earlier to the 500BC. The first recorded instance for encryption was around 500BC, named spartan encryption. The techniques used scytale, an invention that allowe d transferring secret messages. In the modern world, companies use various encryption techniques to transfer data by maintaining its integrity. We have researched and mentioned here some of the widely used encryption techniques. The research will help others to select from the mentioned techniques to enhance the security of their data in the application.

We found some issues during this research and have given specific answers from our perspective. Issues that we find make the current algorithm very difficult to implement in modern technology like the internet of things. Some problems are like consuming more memory, which does not make it an ideal choice for low -end devices like Arduino, esp32, etc.

Despite being the oldest and most secure encryption method, DES has been the subject of debates on how long is too long. Diffie and Hellman suggested that although while the effective key length of DES is 56 bits, under certain conditions, the algorithm's symmetric properties may reduce this number in half, meaning that on average only half of these would need to be tested in order to identify the right key. [7]

AES, NIST began work on the AES, which is the recognised successor to DES, in 1997. AES (Advanced Encryption Standard), which demands a lot of processing power, cannot often be implemented on hardware like microcontroller s. We discovered that increasing the number of rounds makes AES more computationally or electrically demanding. As a result, with this approach, the text is simply encrypted using a mathematical equation without the usage of rounds.

Many algorithms, like the Caesar cipher, can easily decrypt as a hacker can easily recognize the pattern. Though they are very lightweight, if not secured cannot be used. To provide a solution to the problem with the non-repetitive cipher text. Here my preference is to point out a situation where a hacker takes advantage of a pattern. This algorithm pattern cannot be identified as it is protected with two layers. We use a mathematical equation that changes the ASCII codes so that patterns cannot be identified. And the second layer of protection is a 10k array of emojis, which is only known to the company and is encrypted with rail-fence cipher. [6]

According to the investigations, the Threefish algorithm is the most advanced one available for use in network communication encryption. Triple Blowfish was discovered to be extremely safe and to maintain the highest level of data security in networks duri ng a test that was done. [8]

We also find that today's many algorithms, including AES and others, are vulnerable to key. Meaning that if the key is known to the attacker, an attacker can easily decrypt the message or data if he somehow gets the key. We provide a solution to this problem by creating a second layer of protection with our 10k array encrypted with rail -fence cipher as an extra layer of protection.

Now let's talk about our Madkem algorithm. You can understand this algorithm by its name itself. MADKEM(Matrix Addition Division Key Management). Here we have created a simple logic of Adding and dividing matrix with a dual key system.

Now let's talk about our objectives: -

1. To Provide a secured solution for encryption and decryption
2. To provide a lightweight solution.
3. To provide dual-layer protection, it's secure if the key is also gone.
4. To come up with a new modern approach to the crypto algorithm.
5. To give a very feasible solution to crypto problems.

Methodology

Many encryption technologies are used widely across the world to encrypt data. The primary purpose of these encryption technologies is to make sure that the integrity of data being transferred stays maintained. These encryption technologies can be categorized into Symmetric Key Encryption and Asymmetric Key Encryption. In Symmetric Key Encryption, the same key is used to encrypt and decrypt the data. Whereas, in Asymmetric Key Encryption, two keys are used, such as the public and private keys, to encrypt and decrypt the data. Some widely used technologies include AES, DES, RSA. Also, there are some additional encryption types, such as Twofish, Blowfish, and Three fish. Let us dig deep into them.

Advanced Encryption Standard (AES)

One of the most crucial parts of any encryption technique is its security. The techniques must be secure enough that they cannot be breached easily and assures data safety. AES was to improve the security issue of the DES algorithm. In AES, mainly, there are three different types of key sizes used.
128-, 192-, or 256-bit key sizes are what AES uses to encrypt and decrypt the data. Also, to be specific, these key sizes decide the number of rounds during the encryption or the decryption. For
128 bit 10 rounds, 192 bit 12 rounds, and 256 bit 14 rounds. [2]

Data Encryption Standard (DES)

Calling it the earliest and the most secure encryption technique will not be wrong today. As it is known, DES is the earliest known block cipher. This earliest known block cipher is based on symmetric key algorithms. The process of encryption and decryption in DES is quite simple to understand. After the launch of DES, the algorithm became the widely used encryption technique around the globe at the timeframe. Also, today, many companies and financial service agencies depend entirely on the DES standard. Furthermore, it can easily be cracked, which is why DES is not so widely used. DES is a symmetric technique because the DES algorithm uses the same binary key for encryption and decryption of the data blocks. [1]

- **Triple Data Encryption Standard (3DES)**

As the name suggests, 3DES is the enhanced form of the DES algorithm. 3DES was first published in
1998. As its ancestor, 3DES is also a block cipher-based symmetric algorithm that uses the same key
for encryption and decryption. In 3DES, the input text is undoubtedly the same as DES, the plaintext
cipher of 64bit. The difference comes from the process of encryption. Instead of one complete process of DES, 3DES goes through DES three times to enhance security. This is the step that differentiates the 3DES from the original DES algorithm. [1]

Rivest-Shamir-Adleman (RSA)

RSA is also a widely used Encryption technique. RSA is a Public-Key algorithm making it an asymmetric algorithm as the asymmetric algorithm means that it requires two keys for the encryption and decryption. The RSA algorithm consists both private and public keys for transmission. So, one key (public key) can be given to anyone without hesitation because the public key's encrypted data can be decrypted only by the given private key. As the keys are the essential part of this algorithm, the key generation part is the most challenging part here, which makes it the most secure algorithm. [4]

Blowfish

Blowfish is an enhanced encryption technique. Blowfish is a block-cipher-based technique that encrypts the data of 64 bits at a time. It uses keys of various lengths, including 32-bit to 448-bit. Blowfish is not an iterative but a Feistel cipher. To be specific, the technique encrypts the data in 16 rounds of operations. [1]

Twofish

Twofish is an advanced form of Blowfish. It is a highly-flexible and symmetric cipher-based algorithm.

As the Blowfish successor, it uses the same 16 rounds process for encryption. For the key, Twofish uses the key with a size of 128,192- or 256-bit size. Specifically, in encryption, only half of the key is used as an actual key. The other half is used for modifying the encryption algorithm. [1]

Threefish

Another symmetric block cipher method is Threefish. Threefish employs an extra key value of 128 bits in addition to the original key importance for all plaintext blocks. Aside from the twofish and blowfish algorithms, the threefish algorithm is highly secure. It encrypts the data using this tweak value. Both the key and the plaintext block have the same size. Data that has a block size of 256 bits,
512 bits, or 1024 bits can be encrypted using Threefish. [1]

Challenges and drawbacks we found for these techniques.

-AES is secure but uses the same process for encrypting every block, which can be easily traced. Also, AES in counter mode becomes very complex to implement in software.
-DES is straightforward and was not designed with a perspective for applications. Which makes it run relatively slow for applications.
-RSA has slow data transfer due to the large number involved.

Our proposed encryption technique – **Madkem**

We have found that the lower bit key could easily get attacked by brute force and cracked. Therefore, we used 256 bits key in this algorithm. Also, if someone can find the key, they may not decrypt the cipher text because the person will need an array of at least 10000 characters or larger defined by that company. Because here, the same key with exact text will have different cipher text.

Steps for Encryption:
1) Create a key of 64 characters that will be converted into ASCII code.
2) The Plain text will be divided into an array of lengths 16 and converted to ASCII code.
3) Key is then divided into 16 sub-array, each containing length of 4 elements.
4) Find out the determinant of each sub-array of the key.
5) Multiply determinant 1 with array 1 of plaintext (we have found in step 2).
6)For instance, Determinant 1 = d1 array 1 = a1
index of array = ia ASCII value = av cipher ASCII = ca
Therefore,
d1*av+(a1*ia) = ca
7. Create a new array of 10k characters with emojis or any text character you want.
8)Take the relative emoji or character from the 10k array according to its index position (index
position = ca).
9. Therefore, you have your ciphertext.

Steps for Decryption
1)convert emoji with its index. Like if ':-)' is in 1024.' :-)' will be converted into 1024
2) av=1024-(a1*ia)/d1
3) convert ASCII to text again

LIMITATIONS

Madkem is an effective encryption technique as you may know by now. The practical implementation of this secure algorithm is yet to be done. We are working on the algorithm to practically implement it.

CONCLUSION

Developers can check out our encryption technique to provide better security and safety. This encryption technique will help secure the user data and the company's confidential data. The Madkem is a complex process, and cracking the algorithm becomes quite hard for hackers.
The Madkem can also be used for cloud encryption. The technique will be quite helpful in securing the data on the cloud and allows for better safety for data. The algorithm provides a strong foundation that will protect data.

REFERENCE

1. Performance Analysis and Evaluation of Cryptographic Algorithms: DES, 3DES, Blowfish, Twofish, and Threefish by HaneenAlabdulrazzaq and Mohammed N.
Alenezi
2. Advanced Encryption Standard (AES) Algorithm to Encrypt and Decrypt Data by Ako Muhammad Abdullah
3. A Study of Encryption Algorithms AES, DES, and RSA for Security By Dr.Prerna Mahajan &Abhishek Sachdeva
4. The RSA Algorithm by SirajuddinAsjad
5. Overview of Modern Cryptography by Kundalakesi Mathivanan
6. Rail Fence Cipher by Daleel Hagy
7. Data Encryption Standard: past and future by M.E. Smid and D.K. Branstad
8. Modern Encryption Techniqes of Communication on Networks by Ali Takieldeen, Rashed Moktar El Awade, and Adel Zaghlol Mahmoud