A Symmetric Key-Based Cryptographic Transaction on Cryptocurrency Data

Tridip Bhowmik[a], Sagir Mahmud Sefat[b], Aysha Akmal[c] and Md. Ismail Jabiullah[d]*

[a] *tridip15-11898@diu.edu.bd*
[a] *Daffodil International University, Sobhanbag, Dhaka 1205, Bangladesh*
[b] *Daffodil International University, Sobhanbag, Dhaka 1205, Bangladesh*
[c] *Daffodil International University, Sobhanbag, Dhaka 1205, Bangladesh*
[d] *Daffodil International University, Sobhanbag, Dhaka 1205, Bangladesh*

Abstract

Cryptocurrency data communications are very demanding issues in current high-speed online currency transactions. Here, a key-based AES (Advanced Encryption Standard) encryption-decryption algorithm is used to impose more security levels on cryptocurrency data communications. For this, the sender first creates a key and sends it to the intended receiver through a secured and trusted channel. Then by that key one can easily encrypt the cryptocurrency data using the AES encryption algorithm and produced the ciphertext and then send it to the destination. On the receiver's end, the decryption process of AES is performed by using the same shared secret key that retrieved the plaintext from the received ciphertext. The security of the proposed process depends on the shared secret key and the algorithm AES and it can be applied for any financial data transactions securely. This can be used in all kinds of cryptocurrency data communication with a higher level of security.

Keywords: Cryptocurrency; AES; Encryption; Decryption; Ciphertext; Security; Transaction; Key;

1. Introduction

Internet becomes a vital role in every sector of the world, at the same time increasing the security of data. The data we transfer from sender to receiver using unprotected way sometimes. Different techniques are used for protecting valuable data in both the private and public sectors also individual data from attackers who want to steal the data. Now cryptography is the most secure and popular technique to secure valuable data from attackers. Cryptography used two important processes which are Encryption and Decryption [1]. The main purpose of cryptography is data confidentiality, integrity, and availability of our valuable information. There are two methods in cryptography where symmetric key cryptography is one of the most used cryptographic processes. Symmetric key cryptography is a type of encryption scheme in which the same key is used both to encrypt and decrypt messages [2]. At the present time, symmetric key algorithms are mostly used as cryptographic techniques in different types of computer systems to increase data security. Advanced Encryption Standard (AES) is one of the finest symmetric key algorithms announced in 2001 by the National Institute of Standards and Technology (NIST) to replace the Data Encryption Standard (DES) [3]. AES has several advantages in security, flexibility, parallel potential, and so on. Nowadays, cryptocurrency has changed the definition of money and transaction. A cryptocurrency is a virtual currency method that is secured by cryptography. The cryptocurrency security issue is high. As a solution researchers introduce blockchain technology for cryptocurrency security. Blockchain has grown rapidly in recent years, but it

cannot reduce the cryptocurrency security issue. Some cryptocurrencies already faced some ransomware attacks by attackers and lost a huge amount of currency.

In this paper, we are applying AES symmetric key algorithm to encrypt all transactions between nodes to protect information from the adversary.

2. Existing System

Many symmetric key models exist in the crypto world and some models are used successfully. This system's main target is how to secure our important data. Muhammet BAYKARA, R. DAŞ, G. TUNA et al 2016 [4], proposed a new algorithm for encrypting confidential data using a symmetric key algorithm. In this algorithm for encryption processes, they converted plaintext into ASCII characters then they multiple it with character values. The secret key is converted into 16 digits binary system in which a decimal value is calculated to find K. Therefore, calculated A using equation:

$$A = ((1/|\sin K|) + (\log 10V)) * 1000000000000$$

Here, A is switched to a binary number system then it built an array. A new array is created by mixing the arrays depending on the value of K, we used mode operation on the new array and the array is mixed another time. Eight digits of the array were gained after array mixing and converted this array to the decimal system. Then, we added the value of k with these decimal values. Finally, we get ciphertext which is created after obtaining ASCII characters of the sums.

After that, the ciphertext is decrypted after the decryption process and the key is taken from the user. At first, the key is converted to ASCII code and the result is converted to sixteen digits binary number system. Every digit is multiplied by the order of the digit to calculate the sum. The output of the sum is K. Then created the text ASCII equivalent and individually subtracted from K. The values are converted to the binary system taking care that they will have 8 digits and an array is built. Again, used reverse mode operation on K-based array's dimension. Then, the array and the mixed array are separated by the inverse of the encryption. Calculate variance(V) using this equation:

$$V = 10\text{^}((A/1000000000000) - (1/|\sin K|))$$

A new array is built after reverse mode operation has been applied to V based on the mixed array's dimension. Sixteen characters from the new array are obtained from the original(plaintext) text.

3. Proposed System

3.1. Methodology

The proposed encryption-decryption method is based on the concept of a symmetric key cryptographic process. Symmetric-key algorithms are cryptographic algorithms that use the same keys for both encryption and decryption [2]. It is also known as a private key algorithm. The sender and the receiver must know this key and use the same secret key. In this proposed model, we used Advanced Encryption Standard (AES)

symmetric key algorithm for Cryptocurrency based data encryption and decryption. In present-day cryptography, AES is widely adopted and supported in both hardware and software [3]. The AES algorithm transforms valuable data and makes it indecipherable to hackers and other individuals attempting to access your data without authorization. To date, any attackers cannot break the AES security and protection system. That's why in this proposed system we prefer to introduce the AES algorithm. In this model, there are two parts sender and receiver. In the sender, part occurred the encryption process and in the receiver, part occurred the decryption process. For symmetric key-based encryption, the sender sends 128bit cryptocurrency data (Name, ID, Hash). This text pass into the AES encryption algorithm for encrypting the data. Here, we use a 128bit secret key for encryption. This key is valuable because if an unauthorized user knows this key hacker can manipulate or theft important data. Therefore, the encryption algorithm generates 128-bit ciphertext. This ciphertext passes on a receiver end. Ciphertext passes on the AES decryption algorithm for decrypting cryptocurrency data. Here need to use the same secret key. Using the secret key we decrypt the ciphertext. Finally, the receiver end gets access to the original plain text that the sender part sends. Cryptanalyst Unable to Decrypt Ciphertext Since it does not have the Secret Keys. Without a secret key, anybody can't modify or shows encrypted and decrypted data.

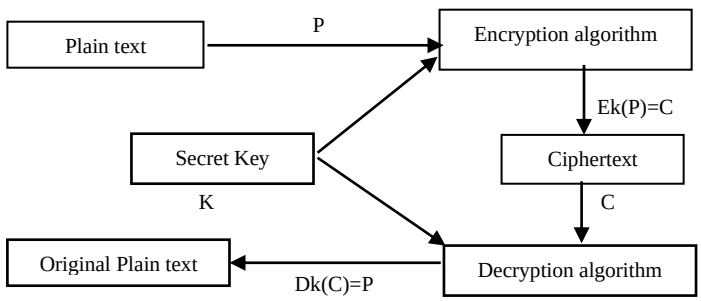

Fig. 1. Encryption-Decryption Process

3.2. Encryption Process

The method of converting the readable plain text into unreadable cipher text using the help of encryption algorithm and the encryption key is called the encryption process [1]. The advanced Encryption Standard (AES) encryption process protect data from attackers. In present days, AES is the most popular and most used symmetric-key algorithm for its security. Till now, any cyber attackers can't break the AES security system. AES algorithm uses a particular structure to encrypt data to provide the best security. AES has three different types of bit lengths and symmetric Keys are used in AES such as AES-128, AES-192, AES-256 bits [1]. Here, in this paper, we used 128-bit standard AES algorithm. The AES cipher is specified as several repetitions of transformation rounds that convert the input plaintext into the final output of ciphertext. Every round build by four different steps such as AddRoundKey, SubBytes, ShiftRows, and MixColumns. The Mixcolumns step is disappear in last round of the process. The rounds in encryption process depend on the size of the key. AES algorithm uses 10 rounds process for 128-bit keys. Now the procedure of encryption process is presented below:

Step 1: The first step of each round is SubBytes transformation [5]. A non-linear transformation of bytes, where each byte substituted from another byte and this substitution completed using an S-box function. The total number of substitution boxes contains a 4x4 matrix and all of the substitution transformations are

completed in only one clock cycle this is called an S-box transformation.

Step 2: The second step of the round is ShiftRow [5]. In this process the first row is unchanged. The next row rotates one byte into shift left. Similarly, the rotation in the third and fourth-row switch left two and bytes respectively.

Step 3: The third step is MixColumn transformation [5]. In this step, we do matrix multiplication Each byte in matrix transformation multiplies with each value of the column. The output of the multiplication are taken place with XOR operation to produce a new four bytes matrix for the next step.

Step 4: The last step is AddRoundKey [5]. AddRoundKey is the key part of the AES algorithm. Here, AddRound key is added to Mixcolumn transformation output by using a simple XOR operation. Each of the rounds has one distinguishable key which is created from the main key. Hence, 10 rounds happen with 11 distinctive keys which came from cipher keys. Then,10 rounds help to encrypt the plain text. Finally, we got ciphertext.
All of this process continues in each round. Only MixColumn doesn't occur in the last round.

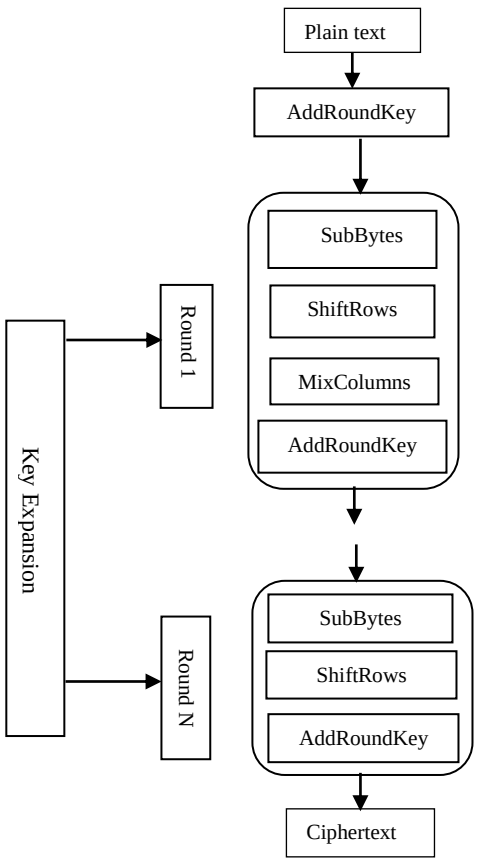

Fig. 2. Encryption Process

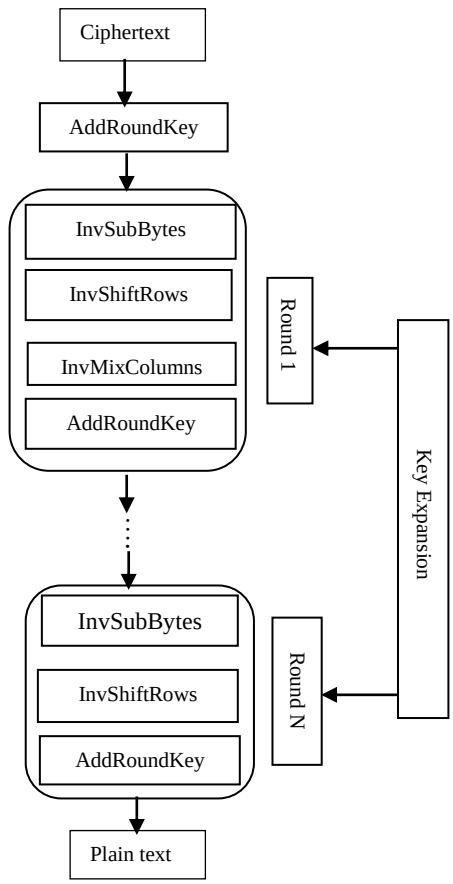

Fig. 3. Decryption process

3.3. Decryption Process

The decryption process converts ciphertext to original plain text using a decryption algorithm and key. In decryption process uses the same key that was received from the sender of the data. The decryption processes of an AES used the inverse mode of the encryption process and use the same key which is used for the encryption process. The decryption steps are inverse SubBytes, inverse ShiftRows, inverse Mixcolumns, and AddRoundKey. In the last round of a decryption technique occurs three steps such as InvShiftRows, InvSubBytes, and AddRoundKey. Mincolumns step is invisible in this round. Here, ciphertext passes into the decryption algorithm and uses the same secret key to decrypt data. After decrypting the data algorithm generate original plain text which is sender sends to the receiver.

4. Implementation

AES algorithm is mostly used and more secure symmetric-key cryptography in the different sectors all over the world. This algorithm is more secure and faster than DES and 3DES symmetric key algorithms. In this paper, we proposed the AES algorithm for secure cryptocurrency data transactions. At first, the user sends plain text (Cryptocurrency Data) to the receiver which is readable. Then used a secure key for the encryption process [Symmetric Key]. The encryption process generates ciphertext which is unreadable. Here encryption process (Fig-4):

Fig. 4. Encryption Process

On the other hand, the decryption process used ciphertext in the AES decryption algorithm and here used the same secret key [Symmetric Key] for decryption. Finally, the receiver gets an original plain text (Cryptocurrency Data) which is a text sent by the sender. Here decryption process (Fig-5):

Fig. 5. Decryption Process

5. Input-Output Analysis

The program of the proposed system has been implemented in the JavaScript programming language for different inputs such as plaintext and different keys and found in different ciphertexts that are presented in the following table.

Plaintext	Key	Ciphertext
Cryptocurrency Data	Symmetric Key	U2FsdGVkX19b1/7J6N9BDyLB/2sVy9dwu7LsArdGH+Zp1HE9Cp75p1DY4R0dxq1
This is Cryptocurrency Data	Symmetric Key 128-bit	U2FsdGVkX1/y76djbE9cRCsLWQdOzUgbDeI1tLO0BStGkRSespb+ARAYmc8UDcbb
Secure Cryptocurrency data	128-bit Symmetric Key$#	U2FsdGVkX18U16kI0DbtIr6Fihqi/grY7km1c1/wYeUQiUSjOkuPNBpAr517p3lQ
Jonathon Nail (P-56464576)	AES-Key-Enc	U2FsdGVkX189OBOB0gyImbHQjXcSbdgBhiJC98RVas6xZK8OrIt5NTlj1dwvzyaL

It is observed that different plaintexts with a different format of keys produce different ciphertexts with different levels of securities. One can easily apply the parameters for their own targeted layer of securities.

6. Comparative Analysis

Now, many researchers develop a new model for secure data transactions. They approach their own idea and want to be more secure rather than the existing model. In this paper, we introduce a new encryption model and explain how it works, its security, and its authentication. Similarly, we study one existing encryption model. How do their model works and we study their algorithm strength and weakness. Finally, we compare the proposed model and the existing model. We consider some properties in both works and show which model fulfills these criteria. There are comparisons between the two models:

Properties	Existing Model	Proposed Model
Authentication	Yes	Yes
Integrity	Yes	Yes
Non-repudiation	Yes	Yes
Speed	Slower	Faster
Time Consumption	High	Low
Complexity	High	Less

7. Conclusion

In the crypto world, the biggest concern is keeping the transaction safe and protected between users. In this paper, we introduce a technique using symmetric key cryptography to secure the cryptocurrency data transaction between two users. Cryptography techniques provide data security using encryption and decryption processes. Here, we propose a method for securely transacting cryptocurrency data between two users using a symmetric key algorithm and we want to ensure the data transaction between two users will be safe. Using this algorithm we can secure any type of data. The proposed algorithm can be passed to achieve

the expected output in the different cryptocurrency fields. This algorithm can ensure data high security, authenticity, and data weakness. Hence, this algorithm can help secure data transactions.

Acknowledgements

I would like to thank the professor of Daffodil International University Dr. Md. Ismail Jabiullah for supporting and suggesting the idea of this research. He reviews this paper.

References

[1] S. Suguna, Dr. V. Dhanakoti, R. Manjupriya. (2016). "A STUDY ON SYMMETRIC AND ASYMMETRIC KEY ENCRYPTION ALGORITHMS". International Research Journal of Engineering and Technology (IRJET), Volume: 03, Issue: 04, Apr-2016.

[2] A. Anand, A. Raj, R. Kohli, Dr. V. Bibhu. (2016). "Proposed Symmetric Key Cryptography Algorithm for Data Security". 1st International Conference on Innovation and Challenges in Cyber Security (ICICCS 2016), IEEE,2016.

[3] S. Chandra, Siddhartha B., Smita, Sk Safikul. "A Study and Analysis on Symmetric Cryptography". IEEE-32331.

[4] M. BAYKARA, R. DAŞ, G. TUNA. (2016). "A Novel Symmetric Encryption Algorithm and its Implementation". Turkish Journal of Science & Technology, Volume 12 (1), 5-9, 2017.

[5] Abdullah. (2017, June). "Advanced Encryption Standard (AES) Algorithm to Encrypt and Decrypt Data".

[6] H. Abroshan. (2021). "A Hybrid Encryption Solution to Improve Cloud Computing Security using Symmetric and Asymmetric Cryptography Algorithms". (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 12, No. 6, 2021.

[7] A. Murtaza, S.J.H Pirzada, Liu Jianwei. (2019). "A New Symmetric Key Encryption Algorithm With Higher Performance". International Conference on Computing, Mathematics and Engineering Technologies – iCoMET 2019.

[8] M.U. Bokhar, Q.M. Shallal. (2016). "A Review on Symmetric Key Encryption Techniques in Cryptography". International Journal of Computer Applications (0975 – 8887), Vol.147, No.10, August 2016.