MULTI-LAYER ENCRYPTION ALGORITHM

Akula Vamsi Krishna Rao[1], V.N. Aditya Datta Chivukula[2],
Sri Keshava Reddy Adupala[2] and Abhiram Reddy Cholleti[3]

[1]Department of Computer Science and Engineering,
CMR Engineering College, Medchal, India
[2]Department of Computer Science and Engineering,
International Institute of Information Technology, Bhubaneswar, India
[3]Department of Electronics and Telecom Engineering, International Institute of Information Technology, Bhubaneswar, India

ABSTRACT

In recent years, security has become a big issue for many applications to defend attacks from intruders. Exchanging credentials in plaintext might expose it to stealers. Many techniques are required to protect the data of the consumers from attackers. Cryptography has come up with a solution to provide security for the users to exchange data securely by the means of the process called as Encryption/ Decryption. In this field, there are basically two techniques of cryptography i.e Symmetric and asymmetric, developed to achieve a secure connection between the sender and receiver. These techniques provide specific goals in maintaining privacy by converting original message to non-readable form and sends it over a communication channel. The unauthorized members try to break the non-readable form but the difficulty depends upon the techniques that were used to encrypt the data. In this paper, we proposed a quadruple encryption algorithm consists of novel phase-shift algorithm, AES (Advanced Encryption Standard), TwoFish and RC4 and making it hard to attack by common methods.

KEYWORDS

Cryptography, AES, Two-fish, RC4, Phase-shift.

1. INTRODUCTION

Cryptography is the process of converting a normal plaintext to unreadable text in the form of using different algorithms [1]. It can be used for authentication, protecting data from criminal which stands against them by locking the particular data using the key. Cryptography involves: Plaintext, Encryption Algorithm, Ciphertext, Decryption algorithm, Encryption key and Decryption key.

Cryptography can provide the following services:

- Confidentiality
- Integrity
- Authentication
- Non-repudiation

David C. Wyld et al. (Eds): VLSIA, INWES, CSIP, BMLI - 2021
pp. 15-21, 2021. CS & IT - CSCP 2021 DOI: 10.5121/csit.2021.112103

Types of Cryptography:

- Symmetric Key Cryptography: It consists of only one key which is used for both encryption and decryption. Symmetric Key consists of Block and Stream algorithms [2]. Some examples of symmetric encryption algorithms include: Advanced Encryption standard (AES), Data Encryption Standard (DES), Blowfish, RC4(Rivest Cipher 4), RC5(Rivest Cipher 5), RC6(Rivest Cipher 6).
- Asymmetric Key Cryptography [2]: It consists of 2 keys which is public key and private key. if message(m) is encrypted with public key then the encrypted text is decrypted using the private key. Some examples of Asymmetric encryption algorithms include: Rivest, Shamir, Adleman (RSA), Diffie-Hellman, Elliptic curve Cryptography (ECC), El Gamal.
- Hash Function [3] in cryptography: Message Digest 5(MD5), SHA (Secure hashing algorithm) like SHA-0, SHA-1, SHA-2, SHA-3 and CRC32.

2. ALGORITHM

This section discusses about a novel phase-shift algorithm and three existing encryption algorithms i.e AES, Twofish and RC-4. The architecture of the proposed technique is shown in fig.1 with phase-shift algorithm in the first level, AES in second level, Twofish in the third level, followed by RC-4 and at last again with phase-shift algorithm.

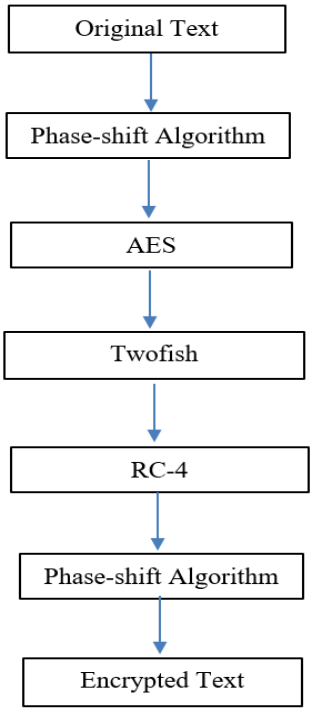

Figure 1. Encryption Process

At each level, the encrypted text is passed to its next level of encryption and the key that is used to encrypt, is stored in a separate array.

For instance, a message is given as an input in the first level. Here, the message gets encrypted and it is passed to the second level. The key that is used to encrypt the message is stored in an array (A1). Now, the second level encrypts the output of the first level i.e encrypted text by first level and stores the key (second level) in the array (A1). Later, the output of the second level is given as an input to the third level. This process is continued till the fifth level.

The previous 5 levels have different set of keys, and the entire set of keys are stored in the form of an array and attached at the end of the data resultant array after four levels of transformations or encryptions. This augmented array is undergone through the final phase shift. Hence, until the angle is known, we cannot perform the inverse phase-shift correctly and thereby, cannot even identify the keys of remaining four levels. This ends the security encryption of the data and algorithm in entirety. Similarly, decryption follows the reverse flow of encryption as shown in fig.1.

2.1. Phase-Shift Algorithm

This algorithm [4] is used to rotate an n-dimensional vector by a given angle 'α' (n>=2) having same magnitude, but, with different arrangement of the values. The algorithm basically adopts a dynamic programming approach to perform the task. Initially, it starts with taking the first two dimensions and compares the angle between the original arrangement (first two dimensions) and every arrangement possible keeping the first dimension fixed and adding second dimension in different ways. This process is repeated keeping in view about the cut-off angle is achieved or not. A detailed example is discussed below,

Assume, the initial vector (init_vector) is [1,2,3] and we have to rotate the vector, such that, the rotated vector combination is 90 degrees to the initial. So,

Step 1: let temp_vector = [1] (first dimension of original vector) and α = 0 degrees

Step 2: take second dimension and calculate all possible angles with the original two-dimensional space of vector.
Two combinations that are possible is [1,2] and [2,1]

Case 1: angle between [1,2] and [1,2] is 0 degrees, hence, α_temp = 0 and check if 90>α_temp> α.

If, true, α_temp = α else no change in α.

Case 2: angle between [1,2] and [2,1] is 37 degrees, hence, α_temp = 37 and following previous case, as 90>α_temp > α, α = α_temp.

Step 3: update the temp_vector = [2,1] (vector combination corresponding to greatest α).

Step 4: assign α _temp = 0

take third dimension and calculate all possible angles with the original three-dimensional space of vector.

Three combinations that are possible is [3,2,1], [2,3,1] and [2,1,3].

Case 1: angle between [1,2,3] and [2,1,3] is 21.7 degrees, hence, α_temp = 21.7 and as 90>α_temp> α,

therefore, $\alpha = 21.7$ degrees

Case 2: angle between [1,2,3] and [2,3,1] is 38.2 degrees, hence, $\alpha\_temp = 38.2$ and as $90 > \alpha\_temp > \alpha$.

$\alpha = 38.2$ degrees.

Case 3: angle between [1,2] and [3,2,1] is 44.41 degrees, hence, $\alpha\_temp = 44.41$ and as $90 > \alpha\_temp > \alpha$, $\alpha = 44.41$ degrees.

Vector corresponding to highest angle is [3,2,1] and this is the last iteration, hence, temp_vector = [3,2,1]. The highest angle possible with given combination is 44.41 degrees.

Therefore, if the given angle is not possible, the algorithm rotates the vector to near required angle. This entire algorithm can be used for transmission of arrays of data with key as the angle. This is the first level of security transformation applied to data.

2.2. AES (Advanced Encryption System)

The AES algorithm works on a 128-bit block of data and executed N - 1 loop times. The key length of the algorithm is 128, 192 or 256 bits in length [5,6]. The first and last round of the algorithm has different properties where AddRoundkey is added in first rounds whereas MixColumn is removed in the last round.

Here, we use the AES-128 of 128-bit length key for explanation. The AES Encryption algorithm is broken into 4 categories for operation i.e Sub Bytes, Shift rows, Mix Columns and AddRoundkey. We also do key expansion in the round for cipher key. The separate transforms are performed in a number of rounds that are dependent on the cipher key size. Generally, for key size of 128 we perform 10 rounds, for key size of 196 we do 12 rounds and for 256 we do 14 rounds respectively.

The operation in AES are as follows:

- SubBtyes Transformation: In Sub Bytes transformation bytes are transformed using a non-linear S-box which is invertible. Generally, it is represented as a 16*16 array, where rows and columns are indexed by hexadecimal bits. The corresponding value of the row and column are replaced from the values to it in S-box.
- ShiftRows Transformation: In ShiftRows transformation, the function shifts the bytes in each row of matrix, according to their offsets 0,1,2,3. Let there are 4*4 matrix where four rows are shifted cyclically to left. This is a simple permutation and nothing more.
- MixColumns Transformation: The MixColumn operation is basically a substitution. The byte of a column is mapped into a new value that is function of all bytes in the column. Each element of product is the sum of products of elements of one row and one column.
- Add RoundKey Transformation: In this Stage the 128-bit of state are bitwise XORed with 128-bit of round key. This operation is involved as a column-wise operation between the 4 bytes of state column and one word round key. It proceeds at one column at time. The column matrix is added by the round key word.
- Key Expansion: The AES Key expansion takes as input of a four word i.e. 16 byte key and produces a array of type linear in 44 words i.e. 176 bytes. Each round uses four of these words, where each word contains 32 bytes that means each subkey is 128 bits long.

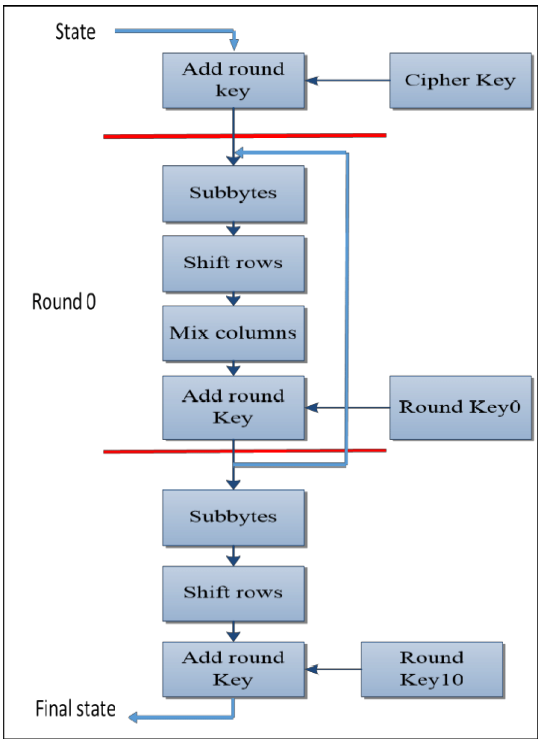

Figure 2. AES Encryption and Decryption

AES Decryption is the reverse process of AES Encryption which inverse round transformations to computes out the original plaintext of an encrypted cipher-text in reverse order. The round transformation of decryption uses the functions Add RoundKey, InverseMix Columns, Inverse Shift-Rows and Inverse Sub-Bytes successively.

- Add RoundKey: Add Roundkey decryption is the operation of inverse transformation of the Encryption.
- Inverse Sub-Bytes transformation: The Inverse Sub-Bytes transformation is done using a once pre-calculated substitution table called InvS-box. That Inverse S-box table contains 256 numbers (from 0 to 255) and their corresponding values.
- InvShiftRows Transformation: Inverse Shift-Rows exactly functions the same as Shift-Rows, only in the opposite direction
- InvMix Columns Transformation: The Inverse Mix Columns transformation is performed using polynomials degree less than 4, which coefficients are the elements in the columns of the state.
- Key Expansion: Key Expansion of AES Decryption is similar to the Key Expansion of AES Encryption.

2.3. Two-fish

Twofish encryption algorithm is a symmetric block cipher which was designed by Schneier in 1998 [7]. Two fish is related to its predecessor block cipher Blowfish. This block cipher considers the block size of 128 bits and key sizes of 128, 192 and 256 bits. This algorithm uses a pre-computed, key-dependent S-box and a relatively complex key schedule [8]. This algorithm was extensively cryptanalyzed and all design elements have a reason. It has 16 rounds Feistel-like structure with additional whitening at the input and output. The basic process of Two fish follows:

- The plaintext is broken up into four 32-bit words and each is XORed with a 32-bit expanded key.
- In each round, two 32-bit words serve as input into the function. Each word is broken up into 4 bytes. Those 4 bytes are sent through four different key-dependent S-boxes.
- The four output bytes are combined using a Maximum Distance Separable (MDS) matrix and combined into a 32-bit word.
- later the two 32-bit words are combined using a Pseudo-Hadamard Transform (PHT). It is added to two round subkeys and then XORed with the right half of the text. There are also two 1-bit rotations going on, one before and one after the XOR.

2.4. RC-4

RC4 is a symmetric cryptographic technique (algorithm) that belongs to the serial cypher (stream cipher) category of symmetric cryptography [9,10]. It's a byte-oriented stream cypher with a variable key length. The RC4 algorithm is distinguished by its simplicity and speed of execution. The key length is also flexible, with a range of 1-256 bytes (8-2048 bits). When the key length equals 128 bits, the violent search key is no longer used, according to current technological support. It's far too likely, thus the RC4 key range should be capable of surviving violent search key attacks for a long period. In fact, there has yet to be discovered an effective attack method for the RC4 encryption algorithm with a 128-bit key length. The key variables in RC4 are

- Key stream: The RC4 algorithm's fundamental feature is that it generates a key stream depending on the plaintext and the key. The length of the key stream and the plaintext are equivalent. That is, the plaintext is 500 bytes long, and the key stream is also 500 bytes long. The encrypted ciphertext is, of course, 500 bytes long, Since the ciphertext i-byte = plaintext i-th byte ^ key stream i-th byte.
- State vector S: The length is 256 characters. S(0), S(1), S(2), S(3), S(4).....S(255), each unit is a byte. Every time the algorithm is run S both contain a set of 8-bit numbers ranging from 0 to 255, with the only difference being the value's position.
- Temporary vector T: Each unit is also a byte, and the length is 256. Assume that the key is 256 bytes long, the key's value is assigned to T directly; otherwise, each byte of the key is assigned to T in turn.
- Key K: The length is 1-256 bytes. It's worth noting that the length of the key keylen isn't always proportional to the plaintext and key stream lengths. The key is usually 16 bytes in length (128 bits).

3. CONCLUSION

The need for secure transmission of data has become the call of the day, and hence, it is very much important to develop new and secure algorithms to increase trust and reliability of the data transmission. The work presented is one such effort towards the need or the cause. We tried to deliver a new way of modelling for secure data transmission and have put forward a new algorithm in combination with the current industry standard algorithms. We are very much looking forward to what the field has got to offer in the future and continue our work in shaping it.

REFERENCES

[1] Delfs, Hans, Helmut Knebl, and Helmut Knebl. Introduction to cryptography. Vol. 2. Heidelberg: Springer, 2002.

[2] Chandra, Sourabh, et al. "A comparative survey of symmetric and asymmetric key cryptography." 2014 international conference on electronics, communication and computational engineering (ICECCE). IEEE, 2014.
[3] Gauravaram, Praveen, and Lars R. Knudsen. "Cryptographic hash functions." Handbook of Information and Communication Security. Springer, Berlin, Heidelberg, 2010. 59-79.
[4] V.N.Aditya Datta Chivukula, Abhiram Reddy Cholleti &Rakesh Chandra Balabantaray, "Lyrics to Music Generator : statistical approach", to appear in Proceedings in International conference on data mining and machine learning (2021).
[5] AES Proposal:Rijandael, Daemen, Joan, and Vincent Rijmen. "AES proposal: Rijndael." (1999).
[6] Supriya, Niranjan, and Mr R. Niranjan. "Realization of AES Encryption and Decryption Based On Null Convention Logic." (2015): 77-81.
[7] Schneier, Bruce, et al. The Twofish encryption algorithm: a 128-bit block cipher. John Wiley & Sons, Inc., 1999.
[8] Bhanot, R. and Hans, R. (2015) A Review and Comparative Analysis of Various Encryption Algorithms. International Journal of Security and Its Applications, 9, 289-306.
[9] T. D. B. Weerasinghe, "Analysis of a Modified RC4 Algorithm," International Journal of Computer Applications, vol. 51, no. 22, 2012.
[10] P. Jindal dan B. Singh, "A Survey on RC4 Stream Cipher," I. J. Computer Network and Information Security, pp. 37-45, 2015.

AUTHORS

Akula Vamsi Krishna Rao is currently an undergraduate student in the Department of Computer Science and Engineering at CMR Engineering College, India. His area of interests is in Cryptography and Offensive Security.

V. N. Aditya Datta Chivukula is currently an undergraduate student in the Department of Computer Science and Engineering at International Institute of Information Technology, India. His area of interest in Machine learning, Deep learning, etc.

Sri Keshava Reddy Adupala is currently an undergraduate student in the department of Computer Science and Engineering at International Institute of Information Technology, India. His area of interests is in Data Analytics, Data Visualization and Machine Learning.

Abhiram Reddy Cholleti is currently an undergraduate student in the Department of Electronics and Telecom Engineering at International Institute of Informational Technology, India. His area of interest is in antenna design and IoT.