International Journal of Future Generation Communication and Networking
Vol. 13, No. 3, (2020), pp. 3434–3439

A Symmetric Key Cryptographic Algorithm with Improving Security in Multi Authority Attribute based Encryption

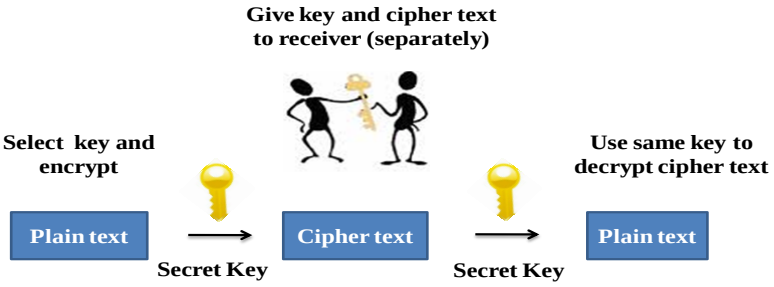
[1]R.Anbhuvizhi [2]A.Jayapradha [3]G. Shobana
[1]Assistant Professor, Department of Science and Humanities, Kumaraguru College of Technology, Coimbatore. Email: anbhuvizhi.r.sci@kct.ac.in
[2]Assistant Professor, Department of Science and Humanities, Sri Krishna College of Engineering and Technology, Coimbatore. Email: jayapradha@skcet.ac.in
[3]Assistant Professor, Department of Computer Science and Engineering, Kumaraguru College of Technology, Coimbatore. Email: shobana.g.cse@kct.ac.in

Abstract

Attribute-based encryption is a type of public-key encryption. The secret key of a user and ciphertext are dependent upon attributes using this type of encryption. Multi authority concept allows any polynomial number of independent authorities to monitor attributes, distribute secret keys and decrypt the message. A symmetric key algorithm is a cryptographic algorithm which is also known as secret key algorithm uses same key to encrypt and decrypt the data. The main idea of this paper is to improve the security issues in multi authority attribute based encryption of a symmetric key cryptographic algorithm.

Cryptography *is a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it. It is the study and practice of hiding information. Cryptography is used in applications present in technologically advanced societies: examples include the security of ATM cards, computer passwords and electronic commerce which all depend on cryptography. There are two basic types of cryptography. Symmetric key and Asymmetric key. Public-key encryption is also referred to as asymmetric encryption and private key is the symmetric key. Private Key is known only to the recipient, used to decrypt messages. Traditional Private-key Cryptography uses one key. It involves using the same key for encryption and decryption. Key is shared by both sender and receiver.*

Private Key Cryptography



ISSN: 2233-7857 IJFGCN

- *In attribute-based encryption, the secret key of a user and the cipher text are dependent upon attributes. The decryption of a cipher text is possible only if the set of attributes of the user key matches the attributes of the cipher text.*

General Terms: *Algorithms, Design, Security.*

Key words: *Cryptography, Network security, Symmetric Key, Attribute based encryption, Cipher text policy.*

1. INTRODUCTION:

To encrypt and decrypt the data, cryptography is the science of using mathematics. It enables to store the sensitive information or transmit it across insecure networks. The concept of securing the messages through cryptography has a long history. Julius Caesar creates one of the earliest cryptographic systems to send military messages. Cryptanalysis is the science of analysing and breaking secure communication. Cryptology embraces both cryptography and cryptanalysis. Attribute Based Encryption (ABE) concept is most widely used to secure the data transmitted through network. In this concept, data or message is encrypted using the attributes of the users and only those users can decrypt the message which is able to satisfied the access structure. Many concepts where introduce regarding security and fast decryption. ABE depends on attributes of the user. Many schemes are developed for ABE using its two policies i.e. key policy ABE and ciphertext ABE.

A cryptographic algorithm or cipher is a mathematical function used in the encryption and decryption process. A cryptographic algorithm works with the combination of keys. The same plaintexts encrypts to different cipher texts with the help of different keys."Cryptography" derives from the Greek word "kryptos" meaning "hidden".

A concept of multi authority was first introduced by Chase in 2007. In that paper, Chase allow any number of authorities t monitor the attributes of the users and distribute secret key. It can also tolerate an arbitrary number of corrupt authorities. When number of user's increases, efficiency of decrypting the ciphertext decreases. So to overcome this problem, the concept of constant ciphertext length was introduced by Emura Keita in 2009. After that many schemes were proposed for constant ciphertext length.

2. CRYPTOGRAPHY:

The plaintext is the data that can read and understand without any special measures. The plaintext is also known as the clear-text. Encryption is the method of disguising plaintext to hide its substance and Decryption is the process of reverting the cipher text into its original plain text. Cryptography is used to achieve the following goals:

2.1. Confidentiality:

Confidentiality ensures no user can read the message except receiver. It is usually achieved through encryption. Encryption algorithms are used to convert plaintext into ciphertext and the decryption algorithms are used to convert the ciphertext into the plaintext.

2.2. Data Integrity:

To ensure data is protected from accidental modification. A hash value is a fixed length numeric value derived from the sequence of data. Digital Signatures are usually applied to hash values. Assuring the receiver that the received message has not been altered in any way from the original is data integrity.

ISSN: 2233-7857 IJFGCN

2.3. Authentication:

To assure that data originates from a particular party. Digital certificates are used to provide authentication. The process of proving one's identity is the authentication.

3. Types of Cryptography:

Cryptography is a process which is associated with scrambling plaintext into ciphertext and then back again. The common types of cryptography are Secret Key Cryptography also known as Symmetric Key Cryptography and Public Key Cryptography also known as Asymmetric Key Cryptography.

3.1. Secret key cryptography:

A single key is used for both encryption and decryption in this type of cryptography. The sender uses the key to encrypt the plaintext and then sends the cipher text to the receiver. The receiver applies the same key which is used by the sender to decrypt the message which the receiver recovers the plaintext. The key must be known to both the sender and the receiver. The biggest difficulty is the distribution of keys.

3.2. Public Key Cryptography:

It involves the uses of key pairs: one private and the one public key. Both are needed to encrypt and decrypt a message or transmission. The owner of key is responsible for securing the key. It is accessible to all users.

4. SYMMETRIC KEY ENCRYPTION:

Secret key cryptographic schemes are generally categorized as being either stream ciphers or block ciphers. Stream ciphers operate on a single bit at a time and implement some form of feedback mechanism so that the key is constantly changing. A block cipher is so-called because the scheme encrypts one block of data at a time using the same key on each block. In general, the same plaintext block will always encrypt to the same ciphertext when using the same key in a block cipher whereas the same plaintext will encrypt to different ciphertext in a stream cipher.

Block ciphers can operate in one of several modes; the following four are the most important Electronic Codebook (ECB), Cipher Block Chaining (CBC), Cipher Feedback (CFB) mode and Output Feedback (OFB). The most common secret-key cryptography scheme used today is the Data Encryption Standard (DES), designed by IBM in the 1970s and adopted by the National Bureau of Standards (NBS).DES is a block cipher employing a 56-bit key that operates on 64-bit blocks.

There are a number of other secret key cryptography algorithms that are also in use today like CAST-128(block cipher), RC2 (block cipher), RC4 (stream cipher), RC5 (block cipher), Blowfish (block cipher), Two fish (block cipher).

5. Related Work

In 2009, Keita Emura et al. [1] propose a CPABE with steady length of ciphertext and consistent length of the quantity of matching processing's. Access structure utilized as a part of this plan is AND gates on multi value attributes.

In 2010, Javier Herranz et al. [2] propose a first collusion-resistance ABE plan which delivers constant size ciphertexts and which concedes sensibly expressive unscrambling policies supports only threshold policy.

ISSN: 2233-7857 IJFGCN

In 2011, Kitak Kim et al. [3] propose a new scheme for chosed ciphertext secure ciphertext policy attribute based encryption scheme with constant size ciphertext and t of n threshold policy. Support threshold policy, constant-size ciphertext and chosed ciphertext security.

In 2011, Junzuo Lai et al.[4] describe the development of ciphertext-policy hiding CP-ABE from attribute concealing internal item PE formally. At that point, it propose a concrete development of ciphertext policy hiding CP-ABE. Uses Non-standard complexity assumptions.

6. NEW SYMMETRIC KEY ALGORITHM

6.1. Encryption algorithm

Step 1: Generate the ASCII value of the letter
Step 2: Generate the corresponding binary value of it.
[Binary value should be 8 digits e.g. for decimal 32 binary number should be 00100000]
Step 3: Reverse the 8 digit's binary number
Step 4: Take a 4 digits divisor (>=1000) as the Key
Step 5: Divide the reversed number with the divisor
Step 6: Store the remainder in first 3 digits & quotient in next 5 digits (remainder and quotient wouldn't be more than 3 digits and 5 digits long respectively. If any of these are less than 3 and 5 digits respectively we need to add required number of zeros in the left hand side. So, this would be the ciphertext i.e. encrypted text). Now store the remainder in first 3 digits and quotient in next 5 digits.

6.2. Decryption algorithm

Step 1: Multiply last 5 digits of the ciphertext by the Key
Step 2: Add first 3 digits of the ciphertext with the result produced in the previous step
Step 3: If the result produced in the previous step i.e. step 2 is not an 8-bit number we need to make it an 8-bit number
Step 4: Reverse the number to get the original text i.e. the plaintext.

7. *Attribute Based Encryption*

Bilinear Group: The security of the CP-ABE scheme depends on the mathematical group called bilinear group, which are group with bilinear map.

Bilinear map: Let G and GT be two multiplicative cyclic groups of prime order p. Let g be a generator of G and $e : GXG \rightarrow GT$ is a bilinear map with following properties:

1. Bilinearity: For all $u, v \in G$ and $a, b \in Z_p$, we have $e(u^a, v^b) = e(u, v)^{ab}$
2. Non-degeneracy : $e(g, g) \neq 1$. If the group operation in G and the bilinear map $e : GXG \rightarrow GT$ are both efficiently computable then it is said that G is bilinear group.

Discrete Logarithm Problem: Given two group elements g and h, find an integer $a \in Z_p$ such that

$$h = g^a \bmod p$$ whenever such integer exist.

8. ADVANTAGES OF THE NEW ALGORITHM

1. The Algorithm is very simple in nature.
2. There are two reverse operations present in this algorithm which would make it more secured.
3. CRC checking in receiving ends is easier
4. For a small amount of data this algorithm will work very smoothly.

Example

Let, the character is "T". Now according to the steps we will get the following:

Step 1: ASCII of "T" is 84 in decimal.
Step 2: The Binary value of 84 is 1010100. Since it is not an 8 bit binary number we need to make it 8 bit

ISSN: 2233-7857 IJFGCN

number as per the encryption algorithm. So it would be 01010100

0	1	0	1	0	1	0	0

Step 3: Reverse of this binary number would be 00101010

0	0	1	0	1	0	1	0

Step 4: Let 1000 as divisor i.e. Key
Step 5: Divide 00101010 (dividend) by 1000(divisor)

Step 6: The remainder would be 10 and the quotient would be 101. So as per the algorithm the ciphertext would be 01000101 which is ASCII 69 in decimal i.e. "E"

0	1	0	0	0	1	0	1

Decryption algorithm
Step 1: Multiply last 5 digits of the ciphertext by the Key

Step 2: Add first 3 digits of the ciphertext with the result produced in the previous step

Step 3: If the result produced in the previous step i.e. step 2 is not an 8-bit number we need to make it an 8- bit number

Step 4: Reverse the number to get the original text i.e. the plain text

9. Our Contribution:

In this paper, a new scheme is proposed that is targeted to achieve multi authorities. The research work is to achieve the multi authorities ABE with fast decryption by applying the concept of symmetric key encryption.

10. CONCLUSION

Cryptography becomes important aspect for transmitting data through network. So to prevent main aspects of security i.e. authentication, integrity, confidential and non-repudiation., there are many algorithms which secure the data transmitted through network. Cryptography is used to achieve few goals like Confidentiality, Data integrity, Authentication etc. of the send data. Now, in order to achieve these goals various cryptographic algorithms are developed by various people. For a very minimal amount of data those algorithms wouldn't be cost effective since those are not designed for small amount of data. The aim of this work was to design and implement a new algorithm to address this issue so that we don't have to apply this algorithm to encrypt a small amount data. The proposed algorithm has been designed in a quite simple manner sacrificing the security issues. A single key is used for both encryption and decryption i.e. it is fallen under secret key cryptographic algorithm. But as public key cryptography is more secured than secret key cryptography, our next task would be to develop and design a public key cryptographic algorithm in a simple manner.

References

1. Emura Keita, Atsuko Miyaji, Akito Nomura, KazumasaOmote, and Masakazu Soshi, "A ciphertext-policy attribute-based encryption scheme with constant ciphertext length.", In *Information Security Practice and Experience*, pp. 13-23, 2009.
2. Herranz Javier, Fabien Laguillaumie, and Carla Ràfols, "Constant size ciphertexts in threshold attribute-based encryption", In *Public Key Cryptography*, pp. 19-34, 2010.

ISSN: 2233-7857 IJFGCN

3. Kim Kitak, Woo Kwon Koo, Jong Hwan Park, and Dong Hoon Lee, "Chosen Ciphertext Secure Ciphertext-Policy AttributeBased Encryption with Constant Ciphertext Length and Threshold Policy."
4. Lai Junzuo, Robert H. Deng, and Yingjiu Li, "Fully secure cipertext-policy hiding CP-ABE", In *Information Security Practice and Experience*, pp. 24-39, 2011.
5. Ge Aijun, Rui Zhang, Cheng Chen, Chuangui Ma, and Zhenfeng Zhang, "Threshold ciphertext policy attribute-based encryption with constant size ciphertexts", In *Information Security and Privacy*, pp. 336-349, 2012.
6. Doshi Nishant, and DeveshJinwala, "Hidden access structure ciphertext policy attribute based encryption with constant length ciphertext",
In *Advanced Computing, Networking and Security*, pp. 515-523, 2012.
7. Doshi Nishant, and DeveshJinwala, "Updating attribute in CP-ABE: A New Approach", *IACR Cryptology ePrint Archive*: 496, 2012.
8. Doshi Nishant, and DeveshJinwala, "Constant Ciphertext Length in CP-ABE", *IACR Cryptology ePrint Archive*: 500, 2012.
9. Doshi Nishant, and Devesh C. Jinwala, "Fully secure ciphertext policy attribute□based encryption with constant length ciphertext and faster decryption", *Security and Communication Networks*, 2013.
10. XU Peng, Yong TANG, Wenbin JIANG, Hai JIN, and Deqing ZOU, "Ciphertext-Policy Attribute-Based Encryption with Short Keys", *Chinese Journal of Electronics* 23, no. 4, 2014.
11. Zhang Yinghui, Dong Zheng, Xiaofeng Chen, Jin Li, and Hui Li, "Computationally Efficient Ciphertext-Policy AttributeBased Encryption with Constant-Size Ciphertexts", In *Provable Security*, pp. 259-273, 2014.
12. S. William, Cryptography and Network Security: Principles and Practice, 2nd edition, Prentice-Hall, Inc., 1999 pp 23-50
13. Computer and Network security by ATUL KAHATE
14. "Introduction to Public-Key Cryptography", an article available at developer.netscape.com/docs/manuals/security/pkin/contents.htm

ISSN: 2233-7857 IJFGCN