CRYPTOGRAPHY AES ALGORITHM – A REVIEW

Sakshi Chatur[1] , Simran Dhandwani[2], Palak Keshwani[3]

[1]BE Student, CSE Department, KITE Raipur(C.G.)

[2]BE Student, CSE Department, KITE Raipur(C.G.)

[3]Assistant professor, CSE Department, KITE Raipur(C.G.)

E-mail - shina9439@gmail.com simmidollzoya33@gmail.com palakeshwani@gmail.com

ABSTRACT

The main aim of this paper is to provide a broad review of network security and cryptography, with particular regard to encryption and decryption algorithm. Network security and cryptography is a subject too wide ranging to cover about how to protect information in digital form and to provide security services. Once the data is out of hand, people with bad intention could modify or hack your data, either to collapse the data or for their own benefit. Cryptography can reformat and transform our data, making it safer on its trip between computer to another computer. If contrasted with the standard bottom-up approach to defining models of computation, algorithms, complexity, efficiency, and then security of cryptographic schemes, our approach is top-down and axiomatic, where lower abstraction levels inherit the definitions and theorems from the higher level, but the definition of low levels is not required for proving theorems at the higher levels. The goal is to strive for simpler definitions, higher generality of results, simpler proofs, diagrams and to derive new insights from the abstract viewpoint.

1.Introduction

Cryptography is associated with the process of converting ordinary plain text into meaningless text and vice-versa. It 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. Cryptography not only protects data from theft or hacker, but can also be used for user verification. Earlier cryptography was effectively synonymous with encryption but nowadays cryptography is mainly based on mathematical theory and computer science practice.

There are some primary functions of cryptography:

1. **Privacy/confidentiality***:* Ensuring that no one can read the message except the exact receiver.
2. **Authentication***:* The process of proving one's identity.
3. **Integrity**: Assuring the receiver that the received message has not been altered in any way from the original.
4. **Non-repudiation***:* A mechanism to prove that the sender really sent this message.

In cryptography, the unencrypted data, is referred to as plaintext. Plaintext is encrypted into cipher text, which will usually be decrypted back into usable plaintext. The encryption and decryption is based upon the type of cryptography scheme being engaged and some differ in the form of the key. This process is sometimes written in formula like:

$$C=E_k(P)$$

$$P = D_k(C)$$

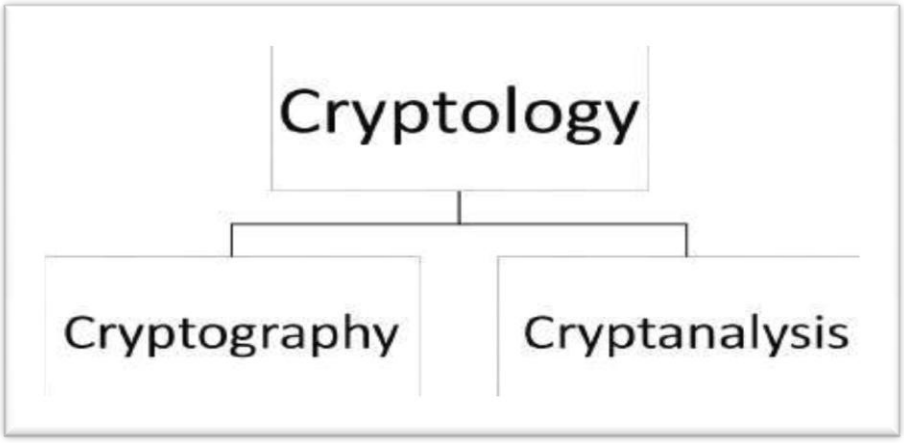
where P = plaintext, C = cipher text, E = the encryption method, D = the decryption method, and k = the key.

Cryptography is most closely associated with the development and creation of the mathematical algorithms used to encrypt and decrypt messages, whereas **cryptanalysis** is the science of analyzing and breaking encryption schemes**. Cryptology** is the term referring to the broad study of secret writing, and encompasses both cryptography and cryptanalysis.

Parts of Cryptography-

Cryptology, the study of cryptosystems, can be subdivided into two kind −

- Cryptography
- Cryptanalysis



Cryptography

Cryptography is the art and science of making a cryptosystem that is capable of providing information security. Cryptography deals with the actual securing of digital data. It refers to the design of mechanisms based on mathematical algorithms that provide fundamental information security services. We can think of cryptography as the establishment of a large tool kit containing different techniques in security applications.

Cryptanalysis

The art and science of breaking the cipher text is known as cryptanalysis. Cryptanalysis is the related branch of cryptography and they both co-exist in network security. The cryptographic process results in the cipher text for transmission or storage. It involves the study of cryptographic process with the intention to collapse them. Cryptanalysis is also used during the design of the new cryptographic techniques to test their security strengths.

Encryption is the process of transforming information so it is unclear to anyone but the intended recipient.

Decryption is the process of transforming encrypted information so that it is clear again. A cryptographic algorithm, also called a cipher, is a mathematical function used for encryption or decryption algorithm. In most cases, two related functions are engaged, one for encryption and the other for decryption. With most modern cryptography, the ability to keep encrypted information secret is based not on the cryptographic algorithm, which is widely known by all, but on a number called a key that must be used with the algorithm to produce an encrypted result or to decrypt previously

encrypted information. Decryption with the correct key is simple. Decryption without the correct key is very difficult, and in some cases impossible for all practical purposes.

The sections that follow introduce the use of keys for encryption and decryption :-

- Symmetric Key Functions.
- Asymmetric Functions.
- Hash Functions.

Symmetric-key Algorithm

Symmetric algorithm's work is to encrypt and decrypt a message using the same key. If we use a key, we can exchange the messages with anybody else using the same key. It is a shared secret. If the key gets in the wrong hands, there is no getting it back. That person can read all of the past messages, and create new messages that are identical from valid data. There are some types of algorithm which are used in previous years:-

- Blowfish
- DES
- 3DES (Triple DES)
- Two fish

But the another algorithm of the symmetric algorithm is the Advanced Encryption Standard(AES) algorithm which is now mostly used to encrypt the messages before passed to the receiver.

1. DESCRIPTION

The Advanced Encryption Standard (AES) algorithm is one of the block cipher encryption algorithm that was published by National Institute of Standards and technology (NIST) in 2000. The main aim of this algorithm was to replace DES algorithm after appearing some unprotected aspects of it.

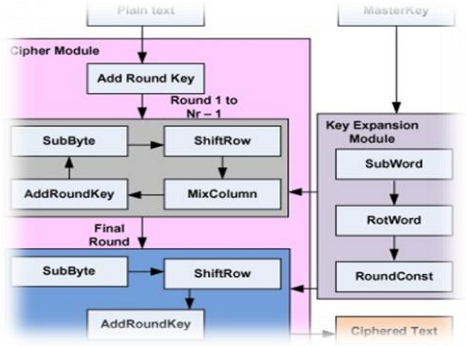


Fig 1. Process of AES algorithm

An implementation of the AES algorithm supports atleast one of the three key lengths: 128, 192, or 256 bits. Implementations may optional support two or three key lengths, which may promote the ability to exchange and use information of algorithm implementations. For the AES algorithm, the length of the Cipher Key, K, is 128, 192 or 256 bits. The key length is represented by nK = 4, 6, or 8 which reflects the number of 32-bit words (number of columns) in the Cipher Key. For the AES algorithm, the number of rounds to be performed during the execution of the algorithm is dependent on the key size. The number of rounds is represented by nR, where nR = 10 when nK = 4, nR = 12 when nK =

6, and nR = 14 when nK = 8. The only Key-Block-Round combinations that conform to this standard are given in the below table.

Bit Pattern	Key Length (nK Words)	Block Size (nB Words)	No.of Rounds(nR Words)
AES-128	4	4	10
AES-192	6	4	12
AES-256	8	4	14

Table1- Key block Round Combination.

For both its *Cipher* and *Inverse Cipher*, the AES algorithm uses a round function that is composed of four different byte oriented transformations :-

1. Byte substitution using a substitution table ,
2. Shifting rows of the State array by different offsets,
3. Mixing the data within each column of the State array, and
4. Adding a Round Key to the State.

Steps of AES Algorithm

2. **Sub bytes**-It is non-linear substitution step where each byte is take place with another according to table.
3. **Shift Rows**-A transposition step where each row of the state is shifted cyclically a such type of number of steps.
4. **Mix Columns**-A mixing operation which operates on the columns of the state, combining the four bytes in each column
5. **Add Round Key**-Each byte of the state is together with the round key; each round key is define from the cipher key using a key process.

AES Applications-

It has many applications. It is used in cases where data is too sensitive and as usally important too that only the authorized person are supposed to know and not to the other person or client. The some of the following are the various applications secure communication :-

- Smart Cards which know mostly used for person identification.
- Using of ATM cards and their networks for using money process.
- Such type of Image encrypt secure storage .
- Confidential co-operate our such important files and documents and some legal Government Documents.
- Personal storage devices in our system or mobiles.
- It saves us person information to the hackers or third party at the time of sharing.

AES Advantages-

Advantages of AES over tripleDES-

- AES is more secure (it is less susceptible to cryptanalysis than tripleDES).
- AES supports larger key sizes than tripleDES's 112 or 168 bits.
- AES is faster in both hardware and software.
- AES's 128-bit block size makes it less open to attacks via the problem than tripleDES with its 64-bit block size.
- AES is required by the latest U.S. and International standards.

Drawbacks of AES

Some drawbacks of AES algorithm:- It uses too simple algebraic structure.

- Every block is always encrypted in the same way.
- Hard to implement with software.

AES in counter mode is complex to implement in software taking both performance and security into considerations.

2.Conclusion

This paper describes the AES algorithm. The encrypted cipher text and the decrypted text are analyzed. The encryption efficiency of the AES algorithm was studied. The algorithm of AES with their advantages and disadvantages was also discussed. The following functions can be categorized for the future of this paper work :-

- An extra modification to be used for 192 bit and 256 bit key AES which is an extension of this paper.
- Power reduction and area minimization is the purpose of the AES algorithm is to be done by the device.

3.Acknowledgement

I would like to thank my guide who gave me an opportunity to share my knowledge about the Cryptography.

4.Referrences

[1]. S. Hirani, “Energy Consumption of Encryption schemes in wireless device Thesis”, university of Pittsburgh, Apr. 9, 2003,

[2]. Nadeem, "A performance comparison of data encryption algorithms", IEEE information and communication technologies, 2006.

[3]. Ravi, S., A., Kocher, P., Hattangady, S.: “Security in embedded systems: Design challenges”. ACM Transactions on Embedded Computing Systems (TECS) 3 (2004) 461-491

[4]. Kocher, P., Lee, R., McGraw, G., A.: Security as a new dimension in embedded system design. In: Proceedings of the 41st annual Design Automation Conference. DAC '04 (2004).

[5]. Kang, K.D., Son, S.H.: Towards security and qos optimization in real-time embedded systems. In: SIGBED Rev. Volume 3., New York, NY, USA, ACM (2006) 29-34

[6]. S. Kim, Ingrid Verbauwhede, "AES implementation on 8-bit microcontroller," Department of Electrical Engineering, University of California, Los Angeles, USA,

