ENCRYPTION PROCESS WITH BLOCK CIPHER & MAC

Pavan A C

Assistant Professor, Department of Computer Science, KLE Society's S.Nijalingappa College, Bengaluru.

ABSTRACT:

Data communication is the most important part of networks that is required between multiple nodes. For data communication securing the data is most important as the data packet can be accessed by any third party. To provide the security for the data an effective AES algorithm technique is utilized. This technique uses multiple rounds and different keys which helps in increasing the complexity to a higher extent and increases efficiency.

Keywords: Advanced Encryption Standard, MAC, Encryption, Decryption.

INTRODUCTION

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. Cryptography is necessary when communicating over any untrusted medium, which includes just about any network, particularly the Internet. In cryptography, we start with the unencrypted data [1], referred to as plaintext. Plaintext is encrypted into cipher text, which will in turn (usually) be decrypted back into usable plaintext.

There are five primary functions of cryptography today:

1. Privacy/confidentiality: Ensuring that no one can read the message except the intended 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.
5. Key exchange: The method by which crypto keys are shared between sender and receiver.

Today's cryptography can be divided into several areas of study, i.e:

- **Symmetric-key cryptography**

Symmetric-key cryptography refers to encryption methods in which both the sender and receiver share the same key. Symmetric key ciphers are implemented as either block ciphers or stream ciphers. A block cipher enciphers input in blocks of plaintext as opposed to individual characters, the input form used by a stream cipher. The Data Encryption Standard (DES) is a symmetric-key algorithm for the encryption of electronic data.

DES is the archetypal block cipher—an algorithm that takes a fixed-length string of plaintext bits and transforms it through a series of complicated operations into another cipher text bit string of the same length. In the case of DES, the block size is 64 bits. DES also uses a key to customize the transformation, so that decryption can supposedly only be performed by those who know the particular key used to encrypt. The key ostensibly consists of 64 bits; however, only 56 of these are actually used by the algorithm. Eight bits are used solely for checking parity, and are thereafter discarded. Hence the effective key length is 56 bits.

- **Public Key Cryptography**

Public key cryptography has been said to be the most significant new development in cryptography in the last 300-400 years. Modern PKC was first described publicly by Stanford University professor Martin Hellman and graduate student Whitfield Diffie in 1976. Their paper described a two-key crypto system in which two parties could engage in a secure communication over a non-secure

communications channel without having to share a secret key. PKC depends upon the existence of so-called one-way functions.

- **Hash Functions**

Hash functions, also called *message digests* and *one-way encryption*, and are algorithms that, in essence, use no key. Instead, a fixed-length hash value is computed based upon the plaintext that makes it impossible for either the contents or length of the plaintext to be recovered. Hash algorithms are typically used to provide a *digital fingerprint* of a file's contents often used to ensure that the file has not been altered by an intruder or virus. Hash functions are also commonly employed by many operating systems to encrypt passwords. Hash functions, then, provide a mechanism to ensure the integrity of a file.

Modern Symmetric Key Encryption

Digital data is represented in strings of binary digits (bits) unlike alphabets. Modern cryptosystems need to process these binary strings to convert in to another binary string. Based on how these binary strings are processed, a symmetric encryption schemes can be classified in to –

- **Stream Ciphers**

In this scheme, the plaintext is processed one bit at a time i.e. one bit of plaintext is taken, and a series of operations is performed on it to generate one bit of ciphertext. Technically, stream ciphers are block ciphers with a block size of one bit.

- **Block Ciphers**

In this scheme, the plain binary text is processed in blocks (groups) of bits at a time; i.e. a block of plaintext bits is selected, a series of operations is performed on this block to generate a block of ciphertext bits. The number of bits in a block is fixed. For example, the schemes DES and AES have block sizes of 64 and 128, respectively.

EXISTING SYSTEM

A Message Authentication Code (MAC) [2-4] is a digital signature that is generated using hash algorithm with the help of a key and some random part of the plain text which is known as MAC-then-Encrypt (MtE) [Fig 1]. That signature will be attached to the message. After the MAC attachment both the Plain text and the MAC will be encrypted. Encryption uses stream cipher scheme to encrypt as well as decrypt. In stream cipher each plain text is encrypted at a time with the corresponding digit of the key stream by XOR operation. Even though stream cipher is fast, the technique is quite simple.

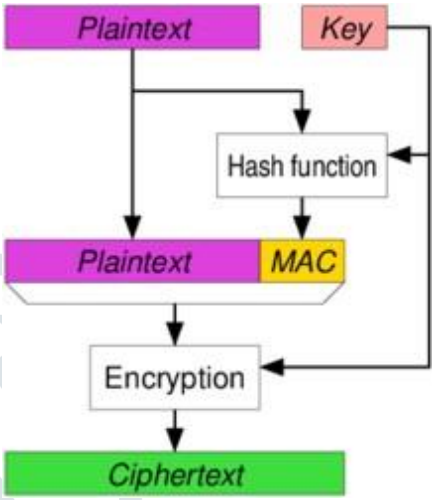

Fig 1: MAC-then-Encryption

As stream cipher is not that secure, after getting through the stream cipher any third party can try and break the MAC using brute force algorithm.

Features of Hash Functions

The typical features of hash functions [5] are –

- Fixed Length Output (Hash Value)
  - Hash function coverts data of arbitrary length to a fixed length. This process is often referred to as hashing the data.
  - In general, the hash is much smaller than the input data, hence hash functions are sometimes called compression functions.
  - Since a hash is a smaller representation of a larger data, it is also referred to as a digest.
  - Hash function with n bit output is referred to as an n-bit hash function. Popular hash functions generate values between 160 and 512 bits.

- Efficiency of Operation
  - Generally for any hash function h with input x, computation of h(x) is a fast operation.
  - Computationally hash functions are much faster than a symmetric encryption.

Disadvantages of Stream Cipher

- Stream ciphers are more difficult to implement correctly, and prone to weaknesses based on usage - since the principles are similar to one- time pad, the key stream has very strict requirements.
- Stream ciphers do not provide integrity protection or authentication.

ENHANCED SYSTEM

The main aim of the enhanced system is to make sure that the wake up time of the system is as less as possible by providing data security. This can be achieved by comparing the integrity of the data using certain algorithms. In the existing system, stream cipher is being used and in this type of process if the cipher text is decrypted then there are more chances of cracking the MAC, so it can be told that encrypt-decrypt process might be crackable. To overcome the drawbacks of stream cipher process it is better to use one of the block cipher scheme that is Advanced Encryption Standard (AES) [7-8] and for the obtained cipher text from AES process MAC signature can be attached.

Advanced Encryption Standard (AES)

AES is relatively a new block cipher based on the encryption algorithm [Fig 2] Rijndael that won the AES design competition. This algorithm is found to be at least six times faster than the one of the famous old block cipher algorithm Digital Encryption Standard (DES) [6].

AES is an iterative cipher. It is based on 'substitution–permutation network' that is it comprises replacing inputs by specific outputs substitutions and others involve shuffling bits around permutations. This algorithm is faster comparatively as it performs all its computations on bytes rather than bits. Hence, AES treats the 128 bits of a plaintext block as 16 bytes. These 16 bytes are arranged in four columns and four rows for processing as a matrix. The number of rounds in AES is variable and depends on the length of the key. AES uses 10 rounds for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys. Each of these rounds uses a different 128-bit round key, which is calculated from the original AES key.

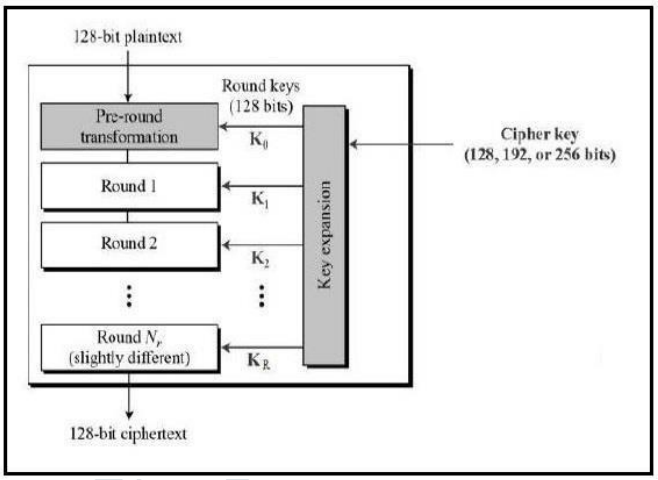

Fig 2: AES Process

Each round comprise of four sub-processes [Fig 3].

- Byte substitution
- Shift rows
- Mix columns
- Add round key

The first round process is depicted below

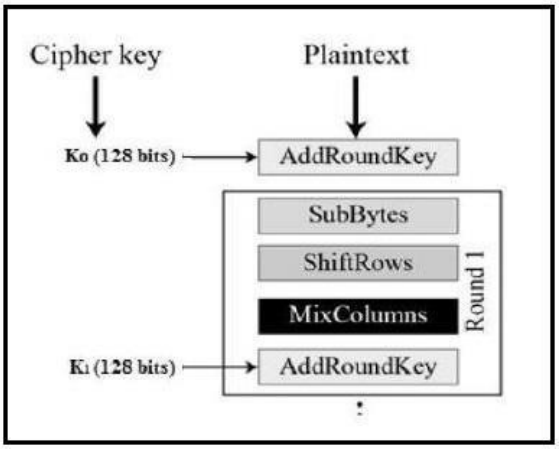

Fig 3: AES Rounds

Byte Substitution (SubBytes)

The 16 input bytes are substituted by looking up to the S-Box rule. The result is in a matrix of four rows and four columns.

Shift Rows

Each of the four rows of the matrix is shifted to the left. Any entries that fall apart are re-inserted on the right side of row. Shift is carried out as follows −

- First row is not shifted.
- Second row is shifted one byte position to the left.
- Third row is shifted two positions to the left.
- Fourth row is shifted three positions to the left.
- The result is a new matrix consisting of the same 16 bytes but shifted with respect to each other.

Mix Columns

Each column of four bytes is now transformed using a special mathematical function. This function takes as input the four bytes of one column and outputs four completely new bytes, which replace the original column. The result is another new matrix consisting of 16 new bytes. It should be noted that this step is not performed in the last round.

Add Round Key

The 16 bytes of the matrix are now considered as 128 bits and are XORed to the 128 bits of the round key. If this is the last round then the output is the cipher text. Otherwise, the resulting 128 bits are interpreted as 16 bytes and we begin another similar round.

After the AES process to make it more secure, hash algorithm is used which uses a key and some arbitrary part of the input message to develop a MAC signature [Fig 4] and it will be attached to the obtained cipher text from the AES process to make it double- encryption.

The process of decryption is comparing the MAC signature, if it compares perfectly then it uncovers the cipher text obtained by AES process and the decrypting process for AES cipher text is as similar to encryption process in the reverse order.

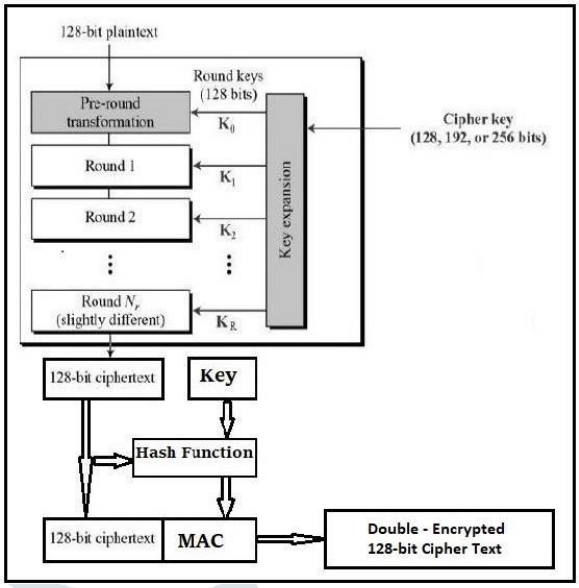

Fig 4: AES-then-MAC Process

Each round comprise of four sub-processes.

- Add round key
- Mix columns
- Shift rows
- Byte substitution

After the above decrypting process the output obtained will the original plain text.

If the MAC does not match, then the receiver system will not wake up, the message will be discarded and AES cipher text will not be available. And on the other hand if the MAC matches and AES fail, even then the receiver system will not wake up and message will be discarded and will not be available.

CONCLUSION

AES Encryption scheme is faster wrt both hardware and software with multiple blocks which becomes more secure and plays an important role in modern cryptography. This technique increases the complexity, which makes the unauthorized party much more difficult to access the data and also no practical cryptanalytic attacks has been discovered till date.

REFERENCES

[1] Pavan A C and P. Prasanna, ―Secure & Energy Efficient Scheme against Denial-of-Sleep Attack in WSN ‖, IJMTST | Volume: 2 | Issue: 05 | May 2016.

[2]A. Bachir, M. Dohler, T. Watteyne, and K. K. Leung, ―MAC essentials for wireless sensor networks,‖ IEEE Commun. Surv. Tuts., vol. 12, no. 2, pp. 222–248, Second Quarter 2010.

[3] J. Kabara and M. Calle, ―MAC protocols used by wirelesssensor networks and a general method of performance evaluation,‖ Int. J. Distrib. Sensor Netw., vol. 2012, pp. 1–11, 2012, Art. ID 834784.

[4] P. Huang, L. Xiao, S. Soltani, M.W. Mutka, and N. Xi, ―The evolution of MAC protocols in wireless sensor networks: A survey,‖ IEEE commun. Surv. Tuts., vol. 15, no. 1, pp. 101–120, First Quarter 2013.

[5] Himanshu Gupta, Vinod Kumar Sharma, ―Multiphase Encryption: A New Concept in Modern Cryptography‖, International Journal of Computer Theory and Engineering, Vol. 5, No. 4, August 2013.

[6] B. Schneier, ―Applied cryptography second edition: protocols, algorithms, and source code in C,‖ John Wiley and Sons, 1996, pp. 758.

[7] M.Pitchaiah, Philemon Daniel, Praveen, ― Implementation of Advanced Encryption Standard in International Journal of Scientific & Engineering Research Volume 3, Issue 3, March - 2012

[8] Advanced Encryption Standard (AES). FIPS. November 23, 2001. http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf (accessed March, 15, 2010).