DES and AES Cryptographic Algorithms: A Review

Anil Kumar

Programmer-Cum-Networking Engineer, Haryana Roadways, Transport Department, Govt of Haryana, India.

ABSTRACT

In recent years network security has become an important issue. Cryptography has been used to secure data and control access by sharing a private cryptographic key over different devices. Cryptography renders the message unintelligible to outsider by various transformations Data Cryptography is the scrambling of the content of data like text, image, audio and video to make it unreadable or unintelligible during transmission. Its main goal is to keep the data secure from unauthorized access.In this paper we are presenting a review of cryptographic algorithms: AES (Advanced Encryption standards) and DES (Data Encryption Standards).

Keywords:AES, DES, Cryptography, Symmetric key, Asymmetric key, Encryption, Decryption

1. INTRODUCTION

Cryptography is a process of hiding information for security purpose. It is the art or science of converting a plain intelligible data into an unintelligible data and again retransforming that message into its original form. Cryptography provides integrity, confidentiality and accuracy. It enables to store sensitive information or transmit it across insecure networks (like the Internet) so that it cannot be read by anyone except the intended recipient. The main goal of cryptography is keeping data secure from the attackers. The process of converting plain text in to unintelligible form (cipher text) is known as Encryption. The process of converting cipher text into plain text is known as Decryption.

2. CRYPTOGRAPHY GOALS

There are five main goals of cryptography. Every security system must provide a bundle of security functions that can assure the secrecy of the system. These functions are usually referred to as the goals of the security system. These goals can be listed under the following five main categories:

- Authentication: The process of proving one's identity. This means that before sending and receiving data using the system, the receiver and sender identity should be verified.
- Privacy/confidentiality: Ensuring that no one can read the message except the intended receiver. Usually this function is how most people identify a secure system. It means that only the authenticated people are able to interpret the message content and no one else.
- Integrity: Assuring the receiver that the received message has not been altered in any way from the original. The basic form of integrity is packet check sum in IPv4 packets.
- Non-repudiation: A mechanism to prove that the sender really sent this message. Means that neither the sender nor the receiver can falsely deny that they have sent a certain message.
- Service Reliability and Availability: Since secure systems usually get attacked by intruders, which may affect their availability and type of service to their users. Such systems provide a way to grant their users the quality of service they expect.

3. TYPES OF CRYPTOSYSTEMS

There are three types of cryptosystems: Symmetric key, Asymmetric key and Hash Functions. Symmetric key encryption uses one key to encrypt and decrypt. Asymmetric key encryption uses two keys; when one key is used to encrypt, the other is used to decrypt. Hash functions create a message digest via an algorithm and use no key.

(a) Symmetric key Encryption Symmetric key (also called private key or secret key) cryptography uses the same key to encrypt and decrypt. The name “private key” derives from the need to keep the key private. A major challenge associated with symmetric key cryptosystems is the secure distribution of keys. Common symmetric key encryption algorithms include DES (the Data Encryption Standard) and AES (the Advanced Encryption Standard).

(b) Asymmetric Key Encryption Asymmetric key encryption (also called public key encryption) uses two keys: a public and a private key. Data encrypted with one key can be decrypted only with the other key. Whitfield Diffie and Martin Hellman first publicly described this approach in November 1976in New Directions in Cryptography, where they announced: “We stand today on the brink ofa evolution in cryptography.”

4. DATA ENCRYPTION STANDARD (DES)

Up until recently, the main standard for encrypting data was a symmetric algorithm known as the Data Encryption Standard (DES). However, this has now been replaced by a new standard known as the Advanced Encryption Standard (AES) which we will look at later. DES is a 64 bit block cipher which means that it encrypts data 64 bits at a time. This is contrasted to a stream cipher in which only one bit at a time (or sometimes small groups of bits such as a byte) is encrypted.DES was the result of a research project set up by International Business Machines (IBM) corporation in the late 1960’s which resulted in a cipher known as LUCIFER. Some of the changes made to LUCIFER have been the subject of much controversy even to the present day. The most notable of these was the key size. LUCIFER used a key size of 128 bits however this was reduced to 56 bits for DES. Even though DES actually accepts a 64 bit key as input, the remaining eight bits are used for parity checking and have no effect on DES’s security. Outsiders were convinced that the 56 bit key was an easy target for a brute force attack due to its extremely small size. The need for the parity checking scheme was also questioned without satisfying answers. Another controversial issue was that the S-boxes used were designed under classified conditions and no reasons for their particular design were ever given. This led people to assume that the NSA had introduced a “trapdoor” through which they could decrypt any data encrypted by DES even without knowledge of the key.

Modes of Operation:

The standard procedure of blocking the message into blocks of length 64 bits and enciphering each block (using the same key) is known as the electronic codebook mode (ECB). It can also be used to produce a key stream cipher; this is known as the output feedback mode (OFB). In this mode of operation, an initialization string of 64 bits is encrypted with DES and then the output is again encrypted, and again, and again ... This produces a bit stream (the original string and each of its encryptions) which is then xor'ed (addition mod 2) with the message to produce the encrypted message as in the one-time pad. Incipher block chaining mode (CBC) the enciphered output of a message block is xor'ed with the next message block before it is run through DES. In this mode of operation, any altered message block will affect all the cipher text blocks that follow it. This is a useful property in certain applications, in particular, in the construction of message authentication codes (MAC's).

Future of DES:

DES was up for a 5 year review by NIST in 1992 and the decision was made to keep it as a standard (to the surprise of many), but at its next review in 1997 it was clear that it was going to be replaced. Some expected it not to remain a standard after this review, but due to NIST's activities concerning the new AES (Advanced Encryption Standard) the decision was made to keep DES as the standard (but only triple DES was to be considered secure). On Dec. 4, 2001, Secretary of Commerce Don Evans announced the approval of AES as the new standard, replacing DES. Products implementing the AES are now available in the marketplace.

Triple DES:

As an enhancement of DES, the3DES (Triple DES) encryption standard was proposed. In this standard the encryption method is similar to the one in original DES but applied 3 times to increase the encryption level. It was used to remove the meet-in-themiddle attack occurred in 2-DES and the brute force attacks in DES. It also has the advantage of proven reliability and a longer key length that eliminates many of the shortcut attacks that can be used to reduce the amount of time it takes to break DES.

5. ADVANCED ENCRYPTION STANDARD (AES)

Since 1977, NIST's Data Encryption Standard (DES) [1] has been the Federal Government's standard method for encrypting sensitive information. In addition, it has gained wide acceptance in the private sector and has been implemented in a wide variety of banking applications. The algorithm specified in this standard has evolved from solely a U.S. Government algorithm into one that is used globally. However, with recent successful key exhaustive attacks, the useful lifetime of DES is now drawing to a close. Anticipating this eventuality, in 1996 NIST officials began preparing for development of a successor standard. In outlining these plans, NIST sought to construct an open process to engage the cryptographic research community and build confidence in the successor algorithm.

On January 2, 1997, NIST announced the initiation of a process to develop the AES [2], which would specify the Advanced Encryption Algorithm (AEA) and serve as an eventual successor to the venerable DES. Basic criteria that candidate algorithms would have to meet were proposed, in addition to required elements in the nomination packages to be submitted to NIST. Over thirty sets of comments were received from U.S. Government agencies, vendors, academia, and individuals. Additionally, NIST sponsored an AES workshop on April 15, 1997 to discuss the comments received and obtain additional feedback to better define the request for candidate algorithms. This input was of great assistance to NIST in preparing its formal call for algorithms and evaluation criteria.

On September 12, 1997, NIST published its formal call for algorithms. [3] Candidate algorithms had to meet three basic requirements: 1) implement symmetric (secret) key cryptography, 2) be a block cipher, and 3) support crypto variable key sizes of 128 bits, 192 bits, and 256 bits with a block size of 128 bits. The algorithm could also support additional key and block sizes. In addition to the above requirements, submitters had to provide the following:

1. Complete written specifications of the algorithm,
2. Statements of the algorithm's estimated computational efficiency,
3. Known answer test values for the algorithm, and code to generate those values,
4. Statement of the algorithm's expected cryptographic strength,
5. Analysis of the algorithm with respect to known attacks,
6. Statement of advantages and limitations of the algorithm,
7. Reference implementation of the algorithm, specified in ANSI C,
8. Optimized implementations specified in Java^TM* and ANSI C, and
9. Signed statements that a) identified any pertinent patents and patent applications and b) provided for the royalty-free use of that intellectual property should the candidate selected be selected for inclusion in the AES.

In its call for candidates, NIST made clear that security would be the most important criterion by which algorithms are evaluated, followed by efficiency and other characteristics. In the spirit of DES success, NIST's goal in the AES development effort is to specify an algorithm that will have a lifetime of at least thirty years, that will be used extensively throughout the U.S. Government, and that will be also be available in the private sector, on a royalty-free basis worldwide.

Twenty-one algorithms were submitted to NIST by the June 15, 1998 deadline. After review, NIST determined that fifteen of these met the minimum acceptability requirements and were accompanied by a complete submission package. These algorithms were made public by NIST on August 20, 1998 at AES1 for the first evaluation period. At the conference, submitters of the fifteen candidate algorithms were invited to provide briefings on the candidates and answer any initial questions. NIST also announced its request for comments on the candidates, due April 15, 1999. These comments will help NIST narrow the field of candidates to approximately five or fewer for the second round of public evaluation. The public analysis of the candidates will be the subject of the Second AES Candidate Conference (AES2), scheduled for March 22-23, 1999. Following its study of the second round analysis, NIST intends to select one algorithm (or possibly more than one, if warranted) to be proposed for inclusion in the AES.

In 2000 the list had been reduced to five finalists: MARS (the IBM entry), RC6 (from RSA Laboratories), Rijndael (from Joan Daemen and Vincent Rijmen), Serpent and Twofish. Eventually

Rijndael was selected to be the AES and the official announcement that it was the new standard was made on Dec. 4, 2001 (to be effective March 26, 2002). Advanced Encryption Standard (AES) : It is a symmetric key encryption standard adopted by the in US government in 2001. It was designed by Vincent Rijmen and Joan Daemena in 1998 later inspected by National Institute of Standards and Technology (NIST) as U.S. FIPS in November, 2001. Various security checks had been performed in the procedure and AES was declared the best encryption standard out of 12 participated standards and the useof AES becomes effective in May, 2002. It has 3 different key sizes: 128, 192 and 256 bits used for the encryption of the 128 bit block size data.

It includes three different default rounds depending upon the key length i.e. 10 for a 128 bit key size, 12 for a 192 bit key size and 14 for a 256 bit key size. The algorithm is designed to use keys of length 128, 192 or 256. It works on one block of 128 bits at a time, producing 128 bits of cipher text. There are 10 rounds, after an initial XOR'ing (bitwise addition mod 2) with the original key (assuming a key length of 128). These rounds, except for the last, consist of 4 steps (layers), called ByteSub, Shift Row, Mix Column and Add Round Key. In the 10th round the MixColumn step is omitted.The 128 bit input is divided into 16 bytes of 8 bits apiece. These are arranged in a 4 × 4 matrix. The ShiftRow and MixColumn steps operate on this matrix while the ByteSub and AddRoundKey steps just operate on the bytes.

6. STRENGTH AND WEAKNESS

Advanced Encryption Standard (AES):

- AES is highly efficient, secure and it is not complex.
- It needs more processing.
- It requires more rounds of communication as compared to DES.

Data Encryption Standard (DES):

- DES has been around a long time since1978 and has been studied to death.even now no real weakness have been found.
- The most efficient attack is still brute force. The 56 bit key size is the biggest defect.
- Hardware implementations of DES are very fast; DES was not designed for software and hence runs relatively slowly.

REFERENCES

[1]. N.Penchalaiah (2010)“Effective Comparison and evaluation of DES and AES.”(International Journal of Computer Science and Engineering)volume 2.

[2]. MajithiaSachin (2010) “Implementation and Analysis of AES, DES and Triple DES on GSM Network.”(International Journal of Computer Science and Network Security), VOL.10.

[3]. Ayushi(2010) “A Symmetric Key Cryptographic Algorithm” (International Journal of Computer Science Applications)Volume1.

[4]. SandipanBasu (2011) “International Data Encryption Algorithm(IDEA)” (Journal of Global Research in Computer Science)Volume2.

[5]. D.kumar,V.Chahar(2011)“Performance Evaluation of DWT based Image Technography.” (IEEE Second International Conference on Advanced Computing).

[6]. S.Pavithra (2012) “ Study and performance analysis of cryptographic algorithms.”(ISSN: 2278 – 1323 International Journal of Advanced Research in Computer Engineering & Technology)Volume 1, Issue 5, July 2012.

[7]. Ajay kakkar(2012)“Comparison of Various Encryption Algorithms and Techniques for secured Data Communication in Multinode Network” (International Journal of Engeneering and Technology) Volume 2 No. ISSN: 2049-3444 © 2011 – IJET.

[8]. Andrew(2012) Cryptography: “A Comparison of Public Key System.”

[9]. ShraddhaSoni (2012)“Analysis and Comparison between AES and DES Cryptographic Algorithm”(International Journal of Engineering and Innovative Technology).

[10]. Nageshkumar (2012) “Performance analysis of symmetric key cryptography. Algorithms: DES, AES and BLOWFISH” (International Journal of Engineering and Innovative Technology) (IJEIT) Volume 2, Issue 6, December 2012 362.

[11]. MohitMarwaha (2013) “Comparative analysis of cryptographic algorithms.”(International Journal of Advanced Engineering Technology) E-ISSN 0976-3945.

[12]. Ali Makhmali(2013)“Comparative Study of Cryptographic Algorithm and Proposing a Data Management Structure”(International Journal of Scientific & Technology)ISSN 2277-8616 Volume 2.

[13]. GurpreetKaur(2013) “ Evaluation and Comparison of Symmetric key.” (International Journal of Science, Engineering and Technology Research) (IJSETR)ISSN: 2278 – 7798 Volume 2.

[14]. Sumitra (2013) “Comparative Analysis of AES and DES security Algorithms.” (International Journal of Scientific and Research Publications), Volume 3, Issue 1, January 2013 1 ISSN 2250-3153