African Journal of Mathematics and Computer Science Research Vol. 3(10), pp. 267-269, October 2010
Available online at http://www.academicjournals.org/AJMCSR
ISSN 2006-9731 ©2010 Academic Journals

Short Communication

The data encryption standard thirty four years later: An overview

Kenekayoro Patrick T.

Niger Delta University, Department of Mathematics/Computer Science, Wilberforce Island, P. M. B. 071, Amassoma, Bayelsa State, Nigeria. E-mail: ktarila@gmail.com.

Accepted 27 August, 2010

The data encryption standard was the first encryption system to meet the National Institute of Standards and Technology's requirements for an encryption system, and also the first standardized encryption system. It was standardized in 1977 and since then, it has been subject to criticisms. The successor to the Data Encryption Standard, Advanced Encryption Standard has been developed and is used today but the Data Encryption Standard is still used today in industries. This paper overviewed the Data Encryption Standard; criticisms faced and concluded if it is still secure enough to protect our confidential information based on published cryptanalysis on this encryption system.

Key words: Block ciphers, TDEA, DES, AES, cryptanalysis, encryption, decryption, cryptography.

INTRODUCTION

The Data Encryption Standard (DES) is one of the oldest symmetric key (same key used to encrypt/decrypt) cryptosystems. The DES was officially standardized in 1976 becoming the first encryption system to meet the National Bureau of Standards (NBS) criteria for an encryption system (Schneier, 1996), and the first standardized encryption system. Thirty four years later, development in cryptography has been enormous and positive changes have been made. The Advanced Encryption Standard (AES) (NIST, 2001) has been developed, new directions in cryptography have been followed; that is asymmetric cryptography (Diffie and Hellman, 1976) (encryption key different from decryption key), even the NBS is now called National Institute of Standards and Technology (NIST).

The DES is still used today; for example it is implemented in the Java cryptography library and is still used in the financial industry. It is also implemented in hardware, for example (Preissig, 2000) is an implementation of the DES on hardware by Texas Instruments. The DES has received its fair share of criticism and has been adapted in several ways to meet current industry standards.

This paper is based on an investigative research on the DES. In the following sections, the basic working principle of the DES, to the scrutiny, adaptation and shortcoming of the DES and Triple Data Encryption Algorithm (TDEA) an extension of the DEA will be described. Finally, it will be determined if the DES is a secure enough encryption system to be used to keep our confidential data safe based on results of the research.

THE DATA ENCRYPTION ALGORITHM

The Data Encryption Algorithm is a symmetric block cipher that encrypts data in 64 bit blocks. It has a key length of 56 bits which is expressed as a 64 bit number; the last bit in every byte acts as a parity check for the previous 7 bits. This is used for error detection.

The three main operations of the DES are: the XOR, permutation and substitution. According to Claude Shannon, encryption of symmetric ciphers comprises confusion and diffusion. The aim of confusion is to make the relationship between the plain text and cipher text complex while diffusion is aimed at spreading the change in the cipher text to hide any statistical feature. In the DES, substitution is used to achieve confusion and permutation diffusion.

Data encryption is also known as "Forward Cipher Operation" and data decryption "Inverse Cipher Operation". In the forward cipher operation, each 64 bit

data (Plain text) are transformed using several mathematical steps (FIBS, 1999) for 16 rounds. The inverse cipher transformation uses the same mathematical steps as the encryption algorithm but we must make sure the same block of key bits used during each round of encryption is used during decryption. That is, where R_{16} L_{16} is the input for decryption, K_{16} is used for that iteration, K_{15} for the R_{15} L_{15}, and so on.

Padding

When the plain text is not a multiple of the symmetric encryption systems block size, we will have an incomplete last block. Extra bits to complete it are added to this incomplete block, thus padding.

A common way to pad is by appending some extra bits to the last plain text block. In 2001, the National Institute of Standards and technology published a recommendation for block cipher modes of operation (Dworkin, 2001). It described padding techniques like the Electronic Code Book (ECB), Cipher Block Chaining (CBC), Cipher Feedback (CFB), Output Feedback (OFB) and Counter (CTR) modes.

To pad, the original DES method appends the message with a single bit followed by as many zeroes to fill out the last block. If the plain text just fills out the last block, then we would have an extra block that is made up of just padded bits. In this method of padding, the cipher text is always longer than the plain text and if this is not desirable in your application, then you would have to use other padding schemes like the Cipher Text Stealing (Daemen, 1995).

In cipher text stealing CTS, if the last block needs to be padded with extra bits, for example 8 bits, it is concatenated with 8 high order bits from the second to the last cipher text block (stealing the cipher text). This complete block is now encrypted and exchanged with the second to the last block. The new last block is then truncated by 8 bits. A proposal was submitted to the National Institute of Standards and Technology to extend the CBC by cipher stealing (CBC-CS). It has not been approved yet but the cipher text stealing padding scheme is widely adopted in many applications.

SECURITY OF DES

The DES algorithm has several weaknesses, for example it has been found that there are four weak keys and 12 semi keys. A weak key is when the DES encryption with key K is inverse to itself (when a plain text is encrypted twice with the weak key the result is the plain text), and keys K1 and K2 are semi weak keys if the DES encryptions with K1 and K2 are inverse to each other. There are only 16 such keys and the DES has a key space of 2^{56} hence the probability of randomly generating a weak or semi weak key is $2^{-52} \approx 2.22 * 10^{-16}$ (Oppliger, 2005) which is very small.

There have been several approaches to attack the DES. The most popular is the linear cryptanalysis (Matsui, 1994) and differential cryptanalysis (Biham and Shamir, 1991). These two approaches reduced the key space needed for search from 2^{56} to 2^{43} and 2^{47} respectively. Other approaches used algebraic cryptanalysis (Courtois and Bard, 2007), molecular computation (Adleman et al., 1999), neural networks (Alallayah et al., 2010), and optimization heuristics (Nalini and Rao, 2006).

A survey (Wiener, 2001) shows the time it takes for cryptanalyst to break cryptographic algorithms. In 1999, a distributed net project broke a DES key in 23 h using exhaustive key search method. The work was shared over 100,000 computers and 250 billion keys were checked every second and a paper (Phan, 2007) shows how to further reduce the exhaustive key search of the DES. At the moment, there is no single system that can check 250 billion keys in a second but it is recommended that keys should be 90 bits long if data must be protected until 2016 (Blaze et al., 1996). We know that the DES key length is only 56 bits as such the DES does not provide the security needed to protect our data.

As a result of these weaknesses, it is advised that the DES should not be used to protect national security systems (Assurance/02-04, CNSS Advisory Memorandum Information, 2005). However, the DES can still be used as a component function of the Triple Data encryption Algorithm (TDEA) (Barker, 2004).

TRIPLE DEA

A TDEA encryption/decryption cipher operation is a compound operation of the DEA encryption/decryption data transformation. A TDEA key consists of three 64 bit keys; these groups of keys (Key1, Key2, and Key3) **(**In TDEA when key1 = key2 = key3, (it is the same as a single DES operation) are collectively referred to as a key bundle.

The forward operation is as follows:

Cipher text 1: the TDEA encrypts the message “m” with Key 1, decrypts it with Key 2, and encrypts it again with Key 3 to create cipher text C.

Similarly, the inverse operation is as follows:

Message $m = D_{k1}\left(E_{k2}\left(D_{k3}(c)\right)\right)$; the TDEA decrypts the cipher text “c” with Key 3, encrypts it with Key 2, and decrypts it again with Key 1 to inverse cipher text C.

NIST specifies the following keying options for a TDEA key bundle (Key 1, Key 2, and Key 3)

1. Keying option 1:Key1, Key2 and Key3 are independent

keys;
2. Keying option 2: Key1 and Key2 are independent keys and Key3 = Key1 (Barker, 2004).

CONCLUSION

There has not been any major successful attack on the DES; its major weakness is its relatively small key length. The only practical attack on the DES exploited this weakness. As faster computers are developed, the security of data encrypted with the DES could be compromised because cryptanalysts could easily break the cipher using brute force (exhaustive key search method).

The DES has been extended to the TDEA to prevent brute force attacks. The TDEA is the encryption system used in industries today, as well as the AES. The DES on its own has been withdrawn by the NIST; its use is only permitted as a component function of Triple Data Encryption Algorithm. The Triple Data Encryption Algorithm is recommended by the US Department of Commerce for protection of unclassified data.

After over thirty years and the development of a new symmetric encryption system (AES), the DES is still secure and used today. Although it is recommended to upgrade to the AES, the transition from DES to AES will be easy as it is not a necessity, hence it will not be rushed. Information secured with the TDEA is still secure.

REFERENCES

Adleman LM, Rothemund PWK, Roweis S, Winfree E (1999). On Applying Molecular Computation To The Data Encryption Standard. University of Southern California; California Institute of Technology.

Alallayah KM, El-Wahed WFA, Amin M, Alhamami AH (2010). Attack of Against Simplified Data Encryption Standard Cipher System Using Neural Networks. 6(1): 29-35.

Assurance/02-04 (2005). CNSS Advisory Memorandum Information, Retirement of Data Encryption Standard. Committee on National Security Systems.

Barker WC (2004). U.S. Department of Commerce, National Institute of Standards and Technology, Recommendation for the Triple Data Encryption Algorithm NIST Special Publication 800-67 version 1.1. National Institute of Standards and Technology.

Biham E, Shamir A (1991). Differential Cryptanalysis of DES-like Cryptosystems. J. Cryptol., 4: 3-72.

Blaze M, Whiteld D, Rivest RL, Schneier B, Tsutomu S, Thompson E, Wiener M (1996). Minimal key Length For Symmetric Ciphers to Provide Adequate Commercial Security.

Courtois NT, Bard GV (2007). Algebraic Cryptanalysis of the Data Encryption Standard. London: University College of London.

Daemen J (1995). Cipher and Hash Function Design, Strategies Based on Linear and Differential Cryptanalysis.

Diffie W, Hellman M (1976). New Directions in Cryptography. IEEE Trans. Inf. Theory, 22(6): 644-54.

Dworkin M (2001). U.S. Department of Commerce, National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation, Methods and Techniques Special Publication 800-38A. National Institute of Standards and Technology.

FIBS (1999). Data Encryption Standard (DES). (FIPS PUB) 46-3. Available from http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf.

Matsui M (1994). Linear Cryptanalysis method for DES Cipher. In Eurocrypt '93. pringer-Verlag.

Nalini N, Rao R (2006). Cryptanalysis of Simplified Data Encryption Standard via Optimisation Heuristics. 6(1B).

NIST (2001). Announcing the Advanced Encryption Standard (AES). Federal Information Processing Standards Publication 197.

Oppliger R (2005). Contemporary Cryptography. Boston / London: Artech House.

Phan RCW (2007). Reducing the exhaustive key search of the Data Encryption Standard (DES). Comput. Standards Interfaces, 29(5): 528-30.

Preissig RS (2000). Data Encryption Standard (DES) Implementation on the TMS320C6000. Texas Instruments.

Schneier B (1996). Applied Cryptography. New York, Chichester, Brisbane, Toronto, Singapore: John Wiley & Sons, Inc.

Wiener M (2001). Brute force attacks on cryptographic keys. [Online] Available at: HYPERLINK "http://www.cl.cam.ac.uk/~rnc1/brute.html" http://www.cl.cam.ac.uk/~rnc1/brute.html [Accessed 25 July 2010].