An Overview of the Data encryption standard (DES)

Manjula .M

Abstract:

As computing power becomes faster and cheaper, cryptographic methods that were reliable and secure yesterday become less so today. In 1977, the Data Encryption Standard was adopted which 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. Since 1977 it has been subject to criticisms that it is insecure. Advanced Encryption Standard (AES) which is the successor of the Data Encryption Standard has been developed which provides more security in the long term but still the Data Encryption standard is used in industries today. 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.

Keywords— **AES, Block ciphers, cryptanalysis, cryptography, decryption, DES, encryption, TDEA.**

I. INTRODUCTION

The Data Encryption Standard (DES) is one of the oldest symmetric-key methods of data encryption. DES works by using the same key to encrypt and decrypt a message, so both the sender and the receiver must know and use the same private key. The DES symmetric-key algorithm for the encryption of data has been replaced the more secure Advanced Encryption Standard (AES) algorithm that is asymmetric cryptography [9] (encryption key different from decryption key),. Originally designed by researchers at IBM in the early 1970s, DES was adopted for the encryption of commercial in 1977 by the U.S. government. The U.S government approved this first encryption algorithm for public disclosure. This ensured that DES algorithm was used by industries for financial services, where the need for strong encryption is high. This Data Encryption Standard was also used in SIMcards, Smartcard, a wide variety of embedded systems, network devices requiring encryption like modems, boxes and routers.

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.

II. THE DATA ENCRYPTION ALGORITHM

The Data Encryption algorithm is a symmetric block cipher, to encrypt a plaintext message; DES groups it into 64-bit locks. 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. 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 [10] 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 R16 L16 is the input for decryption, K16 is used for that iteration, K15 for the R15 L15, and so on.

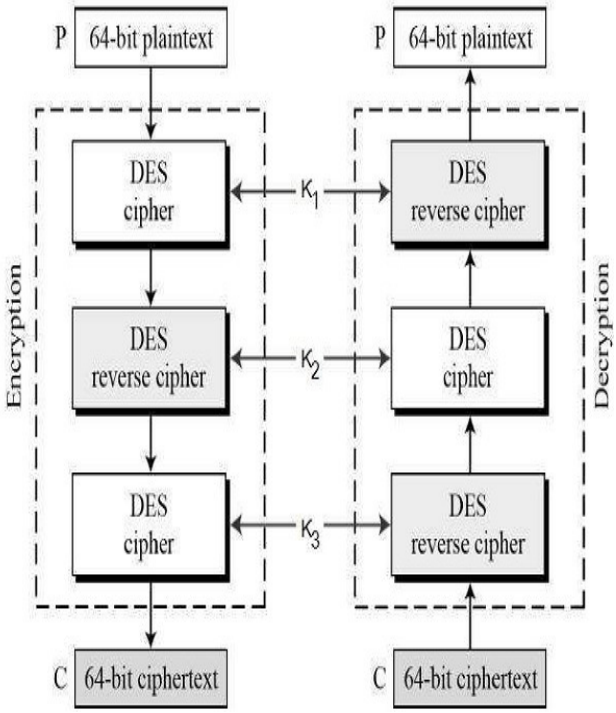
The approved symmetric encryption algorithms: DES, TripleDES, AES. All these algorithms operate on a block of data, typically consisting of 64 bits or 8 bytes, although smaller blocks are also possible. Each block can be processed independently or together with the result of processing on the earlier block, giving rise to different *encryption modes*. The supported modes include ECB (Electronic Cookbook) mode, whereby each block is processed independently, CBC (Cipher Block Chaining) mode, whereby the result of processing the current block is used in processing the next block), CFB (Cipher Feed Back) and OFB (Output Feed Back). The modes like CFB and OFB allow processing with less than 64 bits, with the actual number of bits, usually a multiple of 8, specified after the mode such as CFB8, OFB8, CFB16, OFB16 and so on. The data of these modes like ECB, CBC, CFB16, OFB16 and so on may need to be padded to become a multiple of the block size When a mode requires more than 1 byte to do the processing Bundled providers support PKCS5Padding and also the modes CBC, CFB and OFB need an 8-byte *Initialization Vector*, so that even the first block has an input to start with. This must be same for both encryption and decryption.

III. DATA ENCRYPTION STANDARD SECURITY

There have been several approaches to attack the DES. The most popular is the linear cryptanalysis and differential cryptanalysis [4]. These two approaches reduced the key space needed for search from 2^{56} to 2^{43} and 2^{47} respectively. A survey 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 [14] 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 [5]. 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).

IV. TRIPLE DEA (TDEA)

Triple DES (3DES), officially the Triple Data Encryption Algorithm (TDEA or TripleDEA), A TDEA encryption/decryption cipher operation is a compound operation of the DEA encryption /decryption data transformation., which applies this algorithm three times to each data block using three 64-bit keys for an overall key length of 192 bits (the first encryption is encrypted with second key, and the resulting cipher text is again encrypted with a third key). Before using it the user should generate and is attribute a 3TDES key K, which consists of three different DES keys K_1, K_2 and K_3. So the actual 3TDES key has length 3×56 = 168 bits. (it is the same as a single DES operation) are collectively referred to as a key bundleThe encryption scheme is illustrated as follows –



The encryption-decryption process is as follows –

- Encrypt the plaintext blocks using single DES with key K_1.
- Now decrypt the output of step 1 using single DES with key K_2.
- Finally, encrypt the output of step 2 using single DES with key K_3.
- The output of step 3 is the cipher text.
- Again the reverse process is the Decryption. User first decrypt using K_3, then encrypt with K_2, and finally decrypt with K_1.

An encrypt–decrypt–encrypt process takes place because of the Triple DES design, it is possible to use a 3TDES (hardware) implementation for single DES by setting K_1, K_2, and K_3 to be the same value. This provides backwards compatibility with DES. In Second variant of Triple DES, K_3 is replaced by K_1 which is same as 3TDES.User encrypts plaintext blocks using key K_1 at the first, then decrypt with key K_2, and finally encrypt with K_1 again. Therefore, the key length of 2TDES will be 112 bits. Comparatively Triple DES systems are more secure than single DES, but these are very much slower process than encryption using single DES.

V. CONCLUSION

The major weakness of DES is small key length. The practical attack on the DES exploited this weakness. In the present fast generation, as computing power becomes faster the security of the huge data also has become more

important. The crypanalysts could easily break the cipher using brute force (exhaustive key search method) of encrypted data of DES. The DES has been extended to the TDES to prevent Brute force attacks. Both TDEA and AES is the encryption system used in industries today. 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. Though it is recommended to upgrade to the AES, the information is still secure with the TDEA.

REFERENCES

[1]. 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.

[2]. 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.

[3]. A. Kahate, "Cryptography and network security", The Tata McGraw-Hill publishing company limited, New Delhi, (2003).

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

[5]. 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.

[6]. C. Paar, J. Pelzl and B. Preneel, "Understanding Cryptography: A Textbook for Students and Practitioners", Springer Heidelberg Dordrecht, Bochum, (2010).

[7]. C. P. Pfleeger and S. L. Pfleeger, „Security in Computing", Pearson education, Inc., New Jersey .

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

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

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

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

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

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

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

[15]. R. C. Merkel and M. E. Hellman, "On the Security of Multiple Encryption", Communications of the ACM, vol. 24, no. 7, (1981).

[16]. V. K. Pachghare, "Cryptography and information security", PHI 0learning Private limited, New Delhi, (2009).