International Journal of Interdisciplinary Innovative Research & Development (IJIIRD)
ISSN: 2456-236X
Vol. 03 Issue 01 | 2018

Information Security through DES (Data Encryption Standard) Algorithm

Mohit Singh
Department of Computer Science Mumbai Educational Trust College, Mumbai, India

ABSTRACT

DES (Data Encryption Standard) algorithm in information security system is presented in this paper. This algorithm is to be secure for clients and server. The security architecture of the system is designed by using DES algorithm, which eliminates the fraud that occurs today with stolen data. There is no danger of any data send within the system being intercepted, and replaced. The system with encryption is acceptably secure, but that the level of encryption has to be stepped up, as computing power increases. Results in order to be secure the system the communication between modules is encrypted using symmetric key. The algorithm is believed to be practically more secure in the form of "Triple DES".

***Keywords*— Cipher text, Plaintext, Encryption, Decryption.**

1. INTRODUCTION

DES is the block cipher which 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. It is asymmetric encryption technique which means both sender and receiver use a shared key to encrypt and/or decrypt the data. The only problem with this technique is that if the key is knows to others the entire conversation is compromised. In this the block size is 64 bits it also used 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 basically consists of 64 bits however, only 56-bits 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, and it is always quoted as such. Every 8^{th} bit of the selected key is discarded i.e., positions 8, 16, 24, 32, 40, 48, 56, 64 are removed from the 64-bit key leaving behind only the 56-bit key.

2. LITERATURE REVIEW

Secure and secret means of communication has been always desired for in the field of database systems. There is always a possibility of interception by a party outside of the sender-receiver domain when data is transmitted. Modern digital-based encryption methods form the basis of today's world information security. Data Encryption in its earlier days was used by military and government organizations to facilitate secret information but in present times it is used for protecting information within many kinds of civilian system. In 2007 the U.S. government reported that 71% of companies surveyed utilized data encryption or some of their data in transit.

2.1 Data Encryption Standard

- *DES Encryption Algorithm Concept*

The algorithm's overall structure is shown in Fig 1: there are 16 identical stages of processing, termed *rounds*. There is also an initial and final permutation, termed *IP* and *FP*, which are inverses (IP "undoes" the action of FP, and vice versa). IP and FP have no cryptographic significance, but were included in order to facilitate loading blocks in and out of mid-1970s 8-bit based hardware.

Before the main rounds, the block is divided into two 32-bit halves and processed alternately; this criss-crossing is known as the Feistel_scheme. The Feistel structure ensures that decryption and encryption are very

similar processes — the only difference is that the subkeys are applied in the reverse order when decrypting. The rest of the algorithm is identical. This greatly simplifies implementation, particularly in hardware, as there is no need for separate encryption and decryption algorithms.

The ⊕ symbol denotes the exclusive-OR (XOR) operation. The *F-function* scrambles half a block together with some of the key. The output from the F-function is then combined with the other half of the block, and the halves are swapped before the next round. After the final round, the halves are swapped; this is a feature of the Feistel structure which makes encryption and decryption similar processes.

- *How DES works*

Encryption of a block of the message takes place in 16 states or rounds. From the input key, sixteen 48 bit keys are generated, one for each round. In each round, eight so-called S-boxes are used. These S-boxes are fixed in the specification of the standard. Using the S-boxes, groups of six bits are mapped to groups of four bits.

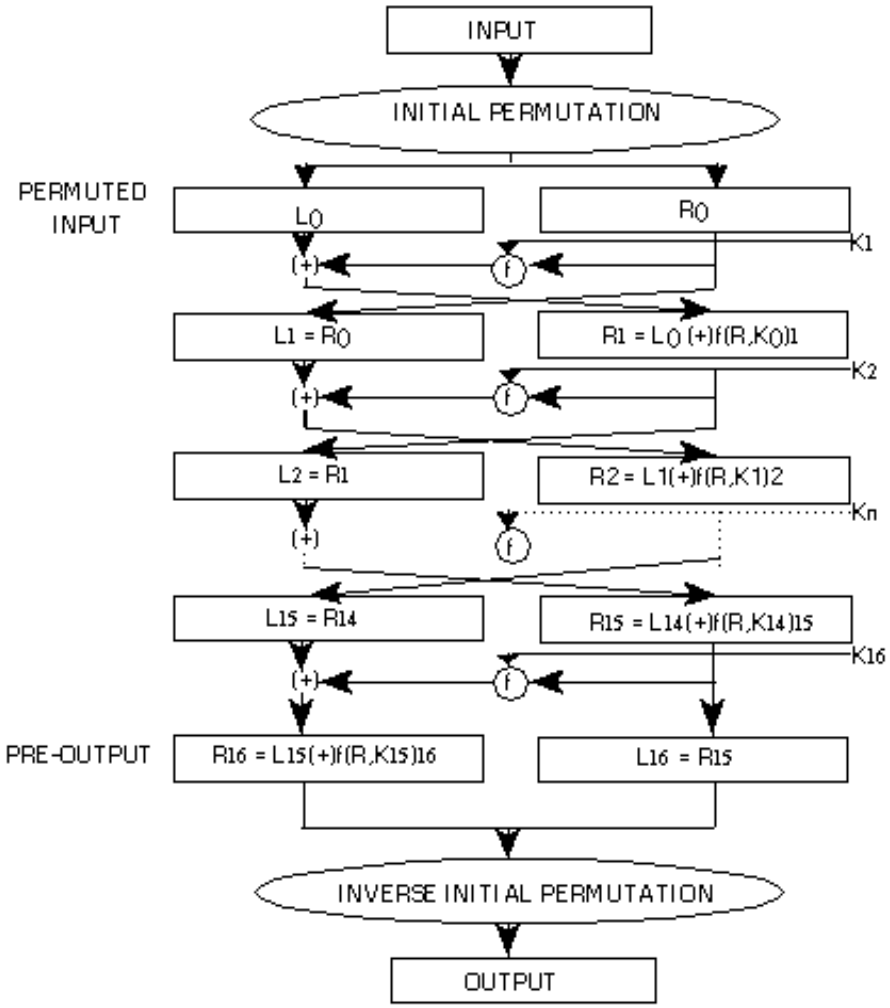

Fig. 1 Working of DES Encryption Algorithm

The contents of these S-boxes have been determined by the U.S. National Security Agency (NSA). The S-boxes appear to be randomly filled, but this is not the case. Recently it has been discovered that these S-boxes, determined in the 1970s, are resistant against an attack called differential cryptanalysis which was first known in the 1990s.

The block of the message is divided into two halves. The right half is expanded from 32 to 48 bits using another fixed table. The result is combined with the subkey for that round using the XOR operation. Using the S-boxes the 48 resulting bits are then transformed again to 32 bits, which are subsequently permutated again

using yet another fixed table. This by now thoroughly shuffled right half is now combined with the left half using the XOR operation. In the next round, this combination is used as the new left half.
The figure should hopefully make this process a bit more clear. In the figure, the left and right halves are denotes as L0 and R0, and in subsequent rounds as L1, R1, L2, R2 and so on. The function f is responsible for all the mappings described above.

- *Why Use Encryption?*

In order to assess the security implications of using DES, it is useful and informative to review the basic rationale for using encryption. In general, we encrypt information because we desire confidentiality. That is, we want to limit access to information, to keep something private or secret. In some cases, we want to share the information within a limited group, and in other cases, we may want to be the sole owner of the information in question. Sometimes, the information we want to protect has value only to the individual, and a loss of confidentiality, while potentially damaging in some limited ways, would typically not be catastrophic. In other cases, the information might have significant financial implications. And in yet others, lives could be at stake. In order to gauge our confidentiality requirements in terms of encryption strength, we must assess the value of the information we are trying to protect, both to us and to a potential attacker. There are various metrics we can employ for this purpose

- ❖ Cost of confidentiality loss
- ❖ Value to adversary
- ❖ Window of opportunity

There are certainly other factors we would consider in conducting a comprehensive security analysis, but these are enough to give a general sense of important questions to answer when evaluating DES as a candidate encryption algorithm.

2.2 Real-World Applications and Threats

Numerous commonly used applications rely on encryption for confidentiality in today's Internet. To evaluate the sufficiency of a given cryptographic algorithm in this context, we should begin by asking some basic questions: what are the real-world risks to these applications, i.e., how likely is it that an application might actually be attacked, and by whom, and for what reasons?

While it is difficult to come up with one-size-fits-all answers based on general application descriptions, we can easily get some sense of the relative threat to many of these applications. It is important to note that what follows is not an exhaustive enumeration of all likely threats and attacks, but rather, a sampling that illustrates that real threats are more prevalent than intuition might suggest. Here are some examples of common applications and related threats:

- Site-to-site VPNs: Often, these are used to connect geographically separate corporate offices. Data traversing such links is often business critical, and sometimes highly confidential. The FBI estimates that every year, billions of U.S. dollars are lost to foreign competitors who deliberately target economic intelligence in U.S. industry and technologies.
- Remote network access for business: See previous item.
- Webmail/email encryption: See Site-to-site VPNs.
- Online banking: Currently, the most common threat to online banking is in the form of "phishing", which does not rely on breaking session encryption, but instead relies on tricking users into providing their account information. In general, direct attacks on session encryption for this application do not scale well. However, if a particular bank were known to use a weak encryption algorithm for session security, it might become worthwhile to develop a broader attack against that bank.
- Electronic funds transfers(EFTs): The ability to replay or otherwise modify legitimate EFTs has obvious financial incentives (and implications). Also, an industrial spy might see a great deal of intelligence value in the financial of a target company.

- Online purchases (E-commerce): The FBI has investigated a number of organized attacks on e-commerce applications. If an attacker has the ability to monitor e-commerce traffic directed to a large merchant that relies on weak encryption, the attacker could harvest a great deal of consumer credit information.
- Internet-based VoIP applications (e.g., Skype): While many uses of this technology are innocuous (e.g., long distance calls to family members), VoIP technology is also used for business purposes (see discussion of FBI estimates regarding corporate espionage above).
- Cellular telephony: Cell phones are very common, and are frequently used for confidential conversations in business, medicine, law enforcement, and other applications.
- Wireless LAN: Wireless technology is used by many businesses, including the New York Stock Exchange. The financial incentives for an attacker are significant in some cases.
- Personal communications (e.g., secure instant messaging): Such communication may be used for corporate communications (see industrial espionage discussion above), and may also be used for financial applications such as stock/securities trading. This has both corporate/industrial espionage and financial implications.
- Laptop hard-drive encryption: See discussion on corporate/industrial espionage above. Also, consider that stolen and lost laptops have been cited for some of the more significant losses of control over sensitive personal information in recent years, notably the Veterans Affairs data loss There are real-world threats to everyday encryption applications, some of which could be very lucrative to an attacker (and by extension, very costly to the victim). It is important to note that if some of these attacks are infrequent today, it is precisely because the threats are recognized, and appropriately strong cryptographic algorithms are used. If "weak" cryptographic algorithms were to be used instead, the implications are indeed thought-provoking.

2.3 Attacking DES

DES is a 64-bit block cipher having a key size of 56 bits. The key actually has 64 bits (matching the block size), but 1 bit in each byte has been designated a 'parity' bit, and is not used for cryptographic purposes. For a full discussion of the history of DES along with an accessible description of the algorithm.

A detailed description of the various types of attacks on cryptographic algorithms is beyond the scope of this document, but for clarity, we provide the following brief descriptions. There are two general aspects of attacks we must consider: the form of the inputs/outputs along with how we might influence them, and the internal function of the cryptographic operations themselves.

In terms of input/output form, some of the more commonly discussed attack characteristics include the following:

- Known plaintext - the attacker knows some of the plaintext corresponding to some of the ciphertext.
- Ciphertext-only - only cipher text is available to the attacker, who has little or no information about the plaintext.
- Chosen plaintext - the attacker can choose which plaintext is encrypted, and obtain the corresponding ciphertext.
- Birthday attacks - relies on the fact that for N elements, collisions can be expected in ~sqrt(N) randomly chosen samples; for systems using CBC mode with random Initialization Vectors(IVs), ciphertext collisions can be expected in about 2^28 samples. Such collisions leak information about the corresponding plaintexts: if the same cryptographic key is used, then the xor of the IVs is equal to the xor of the plaintexts.
- Meet-in-the-middle attacks - leverages birthday characteristic to precompute potential key collision values. Due to the limited scope of this document, these are very brief descriptions of very complex subject matter. For more detailed discussions on these and many related topics.

As for attack characteristics relating to the operational aspects of cipher algorithms, there are essentially two broad classes we consider: cryptanalytic attacks, which exploit some internal structure or function of the cipher algorithm, and brute-force attacks, in which the attacker systematically tries keys until the right one is found. These could alternatively be referred to as white box and black box attacks, respectively.

- Brute-force attacks - In general, a brute-force attack consists of trying each possible key until the correct key is found. In the worst case, this will require 2^n steps for a key size of n bits, and on average, it will require 2^n-1 steps. For DES, this implies 2^56 encryption operations in the worst case, and 2^55 encryption operations on average, if we assume no shortcuts exist. As it turns out, the complementation property of DES provides an attack that yields a reduction by a factor of 2 for a chosen plaintext attack, so this attack requires an average of 2^54 encryption operations.

2.4 Practical Considerations

Above, we described several types of attacks on DES, some of which are more practical than others, but it's very important to recognize that brute force represents the very worst case, and cryptanalytic attacks can only improve on this. If a brute-force attack against a given DES application really is feasible, then worrying about the practicality of the other theoretical attack modes is just a distraction. The bottom line is this: if DES can be brute-force at a cost the attacker can stomach today, this cost will invariably come down as technology advances.

3. DIRECTIONS FOR FUTURE RESEARCH

This paper presents a detailed study of the popular Encryption Algorithm such as DES. The use of internet and network is growing rapidly. So there are more requirements to secure the data transmitted over different networks using different services. To provide the security to the network and data different encryption methods are used. In this paper, a survey on the existing works on the Encryption techniques has been done. To sum up, all the techniques are useful for real-time Encryption. Each technique is unique in its own way, which might be suitable for different applications and has its own pro's and con's. According to research done and literature survey it can be found that DES algorithm is most efficient in terms of speed, time, throughput and avalanche effect. The Security provided by these algorithms can be enhanced further, if more than one algorithm is applied to data. Our future work will explore this concept and a combination of algorithms will be applied either sequentially or parallel, to setup a more secure environment for data storage and retrieval.

4. CONCLUSIONS

As we move toward a society where automated information resources are increasingly shared, data encryption will continue to increase in importance as a security mechanism. Electronic networks for banking, shopping, inventory control, benefit and service delivery, information storage and retrieval, distributed processing, and government applications will need improved methods for access control and data security. The DES algorithm has been a successful effort in the early development of security mechanisms. It is the most widely analyzed, tested, and used encryption algorithm and it will continue to be for some time yet to come. But perhaps the most important contribution of the DES is that it has led us to other security considerations, beyond the algorithm itself that must be made in order to have secure computer systems and networks. We proposed that the data security must be considered to analyze the data security risk, the data security requirements, deployment of security functions and the data security process through encryption. The main contribution of this paper is the new view of data security solution with encryption, which is important and can be used as reference for designing the complete security solution.

5. ACKNOWLEDGMENT

I would like to acknowledge some of the many people who made this work possible. Sincere thanks to my course co-ordinator who guided me Mrs. Chetna Achar for their inspiration, guidance, encouragement and support. Several other researchers also provided data and suggestions along the way.

Many thanks are due to my patient, friends, who endured countless hours of my work towards this goal, and my parents who provided my initial education.

6. REFERENCES

[1] http://www.ukessays.com/essays/security/database-security-and- encryption.php##ixzz2yVjP3N2j
[2] http://en.kioskea.net/contents/134-introduction-to-encryption-with-des
[3] Landau, Susan (March 2000), "Standing the Test of Time: The Data Encryption Standard", *Notices of the American Mathematical Society*.
[4] http://searchsecurity.techtarget.com/definition/Data-Encryption-Standard
[5] http://www.iusmentis.com/technology/encryption/des/
[6] The Design of Rijndael: "AES - The Advanced Encryption Standard" By Sun Song - *Published on Amazon.com*, 28 February 2006.
[7] Matt Curtin "Brute Force: Cracking the Data Encryption Standard", Published by *Springer*, 2007.
[8] Edward F. Schaefer "A Simplified Data Encryption Standard Algorithm" Published by *Taylor & Francis Group*, 04 June 2010.
[9] http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=563518&url= http%3A%2F%2Fieeexplore.ieee.org%2Fstamp%2Fstamp.jsp%3Ftp%3D%26arnumber%3D563518
[10] http://link.springer.com/chapter/10.1007/978-3-642-35326-0_51
[11] http://www.cs.bath.ac.uk/~mdv/courses/CM30082/projects.bho/2004-5/chris_feldwick-2004-5.pdf