www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 3 Issue 12 December 2014, Page No. 9426-9429

Simplified approach towards DES

Harshit Singh, Avineshwar Pratap Singh

B.E., CSE

Takshshila Institute of Engineering and Technology

Jabalpur, M.P., INDIA

B.E., CSE,

Hitkarini College of Engineering andTechnology

Jabalpur, M.P., INDIA

Abstract:

The paper is a short discussion on one of the most important encryption technique ever since it was deduced, this technique utilizes the symmetric key algorithm of Network Security. The symmetric key algorithm is an algorithmwhich makes utilization two keys a public key and a private key so as to limit the data access and thus maintain the much needed secrecy of data.In symmetric key encryption algorithm the private key is the secret key as it rests with the sender and receiver only, this private key is responsible for the secrecy of data. Before we move onto detailed understanding of the algorithm it is necessary to know where is it being implemented or where you will get to see it and the answer to this question is network devices such as modem, routers, bridges, gateway, repeater hubs, and switches and any other device which involves transfer of data that is needed to be kept secret during its transmission to receiver.

About:

Derived out of **Lucifer** one of the developments by IBM in 1970, DES was once a predominant symmetric-key algorithm for the encryption of electronic data and responsible for advancement of

Modern-cryptography,the algorithm was submitted to the National Bureau of Standards (NBS) following the agency's proposal for candidate, for the protection of sensitive, unclassified electronic government data. An NSA-approved encryption standardthat was a slightly modified version of Lucifer by IBM, being strong against differential cryptanalysis, but weak against brute force attacks, andpublished as an official Federal Information Processing Standard (FIPS) for the United States in 1977, resulted in its quick international adoption and widespread academic scrutiny. With controversies starting to arose regardingclassified design elements, short key length of the symmetric-keyblock cipher design, and the involvement of the NSA, started nourishing suspicions about a backdoor. Now considered to be unsecure for many applications, is chiefly due to the too small key size of 56-bit. In January, 1999, distributed.net and the Electronic Frontier Foundation collaborated to publicly break a DES key in 22 hours and 15 minutes.

DES Chronology:

May	1973	NBS publishes a first request for a standard encryption algorithm

August	1974	NBS publishes a second request for encryption algorithms
March	1975	DES is published in the FR for comment
August	1976	First workshop on DES
September	1976	Second workshop, discussing mathematical foundation of DES
November	1976	DES is approved as a standard
January	1977	DES is published as a FIPS standard in FIPS PUB 46
	1983	DES is reaffirmed for the first time
	1986	Video-cipher II, a TV satellite scrambling system based upon DES, begins use by HBO
January	1988	DES is reaffirmed for the second time as FIPS 46-1, superseding FIPS PUB 46
July	1991	Biham and Shamir rediscover DCA, and apply it to a 15-round DES-like cryptosystem.
	1992	Biham and Shamir report the first theoretical attack with less complexity than brute force: DCA. However, it requires an unrealistic 2chosen plaintexts.
December	1993	DES is reaffirmed for the third time as FIPS 46-2
	1994	The first experimental cryptanalysis of DES is performed using linear cryptanalysis (Matsui, 1994).
June	1997	The DESCHALL Project breaks a message encrypted with DES for the first time in public.
July	1998	The EFF's DES cracker (Deep Crack) breaks a DES key in 56 hours.
January	1999	Together, Deep Crack and distributed.net break a DES key in 22 hours and 15 minutes.
October	1999	DES is reaffirmed for the fourth time as FIPS 46-3, which specifies the preferred use of Triple DES, with single DES permitted only in legacy systems.

*Source - Wikipedia

Principle:

The DES encrypts data into 64-bits blocks in a manner that 64-bit of plain text is given as input and 64-bits of cipher text is obtained in output.

Operation:

DES is anarchetypal block cipher algorithm that takes a fixed-length string of plaintext bits transforming it through a series of complicated operations into another cipher-textbit string of block size64 bits. DES 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. Though the key is of 64 bits, only 56 of these are actually used by the algorithm and remaining 8-bits being used solely for checking parity. The effective key lengthof DES is 56 bits, with 8 parity bitswhere each 8-bit byte of the *KEY* may be utilized for

error detection in key generation, distribution, and storage. Bits 8, 16... 64 are for use in ensuring that each byte is of odd parity.DES itself is not a secure means of encryption and hence must instead be used in a mode of operation. FIPS-81 specifies several modes for use with DES, with the comments on usage of DES stated in FIPS-74.

Types:

1.)**Double DES**

Double Data Encryption Algorithm (DDEA or **Double DEA** or **Double DES** or **2DES)** was a quite popular symmetric key block cipher version of DES, it applies the Data Encryption Standard cipher algorithm two times to each data, which means it first performs encryption on plain text using different key and then performs encryption of encrypted text using different key.

2.) **Triple DES**

Triple Data Encryption Algorithm (**TDEA** or **Triple DEA or Triple DES** or **3DES**) is a symmetric-keyblock cipher, which applies the Data Encryption Standard (DES) cipher algorithm three times to each data block. when the algorithm was initially designed the cipher's key size of 56 bits was generally sufficient, but the availability of increasing computational power makingbrute-force attacks more feasible, required NBS to come up with a new and more powerful encryption algorithm, which was triple DES, being improved implementation of original DES and based on basic fundamentals of DES the new algorithm was referred as Triple DES.Triple DES provided a relatively simple method of increasing the key size of DES toprotect against such attacks, without the need to design a completely new block cipher algorithm.

Advantages and Disadvantages:

Advantages:

1.) The key needed for ciphering and deciphering purposes remains the same thus eradicating the burden of new key creation.
2.) Use of different ciphering and deciphering algorithm at two ends, makes it difficult for hackers to pass through using single strategy and requires them to have two different strategies for the two different ends.
3.) Its high speed encryption and decryption capability, was one of the most important feature for its use for over three decades
4.) It is unique because of being supported by most system, libraries and protocols
5.) Permits usage of same hardware or software for decryption as well, with same structure that is used for encryption.
6.) The keys are used in reverse order which means that second key is utilized first and first key is utilized last for decryption purpose.

Disadvantages:

1.) The algorithm is not suitable for enterprise level implementation due to its vulnerability to brute-force attack.
2.) It is slow in speed when compared to many other symmetric key encryption algorithm such as AES, Blowfish, RC4, RC5, and RC6

Verdict:

Though believed to be practically secure in the form of Triple DES, with the possibility of theoretical attacks, DES has been withdrawn as a standard by the National Institute of Standards and Technology (formerly the National Bureau of Standards) and superseded by the Advanced Encryption Standard (AES).

Abbreviations& Definitions:

NBS:

National Bureau of Standards now known as **National Institute of Standards and Technologies**, is a non-regulatory agency of United States department of commerce aimed at promoting US innovations andindustrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life.

DES

The **Data Encryption Standard**, is a symmetric encryption algorithm used for the purpose of secure transmission of data over the network.

FR

An official journal of the federal government of the United States that contains government agency rules, proposed rules, and public notices is known as **Federal Register** (**FR)**. It is published daily, except on federal holidays. The Federal Register is compiled by the Office of the Federal Register (within the National Archives and Records Administration) and is printed by the Government Printing Office. There are no copyright restrictions on the Federal Register; as a work of the U.S. government, it is in the public domain.

FIPS

Standardizations developed by the United States federal government for use in computer systems by all non-military government agencies and by government contractors are known as **Federal Information Processing Standards** (**FIPS**). The purpose of FIPS is to ensure that all federal government and agencies adhere to the same guidelines regarding security and communication.

DESCHALL

The first group to publicly break a message which used the Data Encryption Standard (DES) is referred as **DESCHALL**, and abbreviated form of DES Challenge they became the winner of the first of the set of DES Challenges proposed by RSA Security in 1997. It took them, only 96 days since the announcement of challenge.

EFF's DES

A machine built by the Electronic Frontier Foundation (EFF) in 1998 to perform a brute force on DES, to decrypt an encrypted message by trying every possible key is referred to as **EFF DES cracker**. The aim in doing this was to prove that DES's key was not long enough to be secure. It is also known as **Deep Crack**.

CRYPTANALYSIS

The study of analyzing information systems in order to study the hidden aspects of the systems is **cryptanalysis**.Cryptanalysis is used to breach cryptographic security systems and gain access to the contents of encrypted messages, even if the cryptographic key is unknown., cryptanalysis includes the study of side-channel attacks that do not target weaknesses in the cryptographic algorithms themselves, but instead exploit weaknesses in their implementation.

CRYPTOSYSTEM

Any computer system that involves cryptography for an instance, a system for secure electronic mail which might include methods for digital signatures, cryptographic hash functions, key management techniques, and so on is **Cryptosystem** or **cryptographic system**. Cryptographic systems are made up of cryptographic primitives and are usually rather complex. Because of this, breaking a cryptosystem is not restricted to breaking the underlying cryptographic algorithms - usually it is far easier to break the system as a whole, e.g., through the not uncommon misconceptions of users in respect to the cryptosystem. The systematic arrangement of cypher text can abide the security.

LEGACY SYSTEM

Systems with old method, technology, or application program," of, relating to, or being a previous or outdated computer system and in need of replacement are termed as **legacy system**. Often a pejorative term, referencing a system as "legacy" often implies that the system is out of date.

References:

Books:

1.) Cryptography and Network Security by Atul Kahate
2.) Cryptography and Network Security Principles and Practices by William Stallings.
3.) Guide to Network Security and Principles by Joseph Migga Kizza

Web-Reference:

1.) en.wikipedia.org
2.) www.google.com
3.) www.quora.com