ISSN: 2348 9510

International Journal Of Core Engineering & Management(IJCEM)

Volume 1, Issue 3, June 2014

Implementation Of Hybrid Cryptography Algorithm

Mr. Mahavir Jain
[1]M.E. Student, IET DAVV Indore, M.P.
E-mail id:- e2zinfo@gmail.com

Mr. Arpit Agrawal
Asst. Professor, IET DAVV Indore, M.P.

Abstract

Internet is a public-interacted system; the amount of information exchanged over the internet is completely not safe. Protecting the information transmitted over the network is a difficult task and the data security issues become increasingly important. In recent years, a controversy has arisen over so-called strong encryption. This refers to ciphers that are essentially unbreakable without the decryption keys. While most companies and their customers view it as a means of keeping secrets and minimizing fraud, some governments view strong encryption as a potential vehicle by which terrorists might evade authorities. These governments, including that of the United States, want to set up a key-escrow arrangement. This means everyone who uses a cipher would be required to provide the government with a copy of the key. Decryption keys would be stored in a supposedly secure place, used only by authorities, and used only if backed up by a court order. Opponents of this scheme argue that criminals could hack into the key-escrow database and illegally obtain, steal, or alter the keys. Supporters claim that while this is a possibility, implementing the key escrow scheme would be better than doing nothing to prevent criminals from freely using encryption/decryption. At present, various types of cryptographic algorithms provide high security to information on networks, but they are also have some drawbacks. To improve the strength of these algorithms, we propose a new hybrid cryptographic algorithm in this paper. The algorithm is designed using combination *of two symmetric cryptographic techniques. These two primitives can be achieved with the help of Data Encryption Standard (DES) and International Data Encryption Standard (IDEA). This new hybrid cryptographic algorithm has been designed for better security with integrity.*

Keywords: *cryptography, Encryption, Decryption.*

I. INTRODUCTION

In cryptography, a message authentication code is a short piece of information used to authenticate a message and to detect message tampering and forgery. Here we will study about DES and IDEA algorithms seperately.

1.1 DES

DES is the archetypal block cipher — an algorithm that takes a fixed-length string of plaintext bit and transforms it through a series of complicated operations into another cipher text bit string of the same length. DES also uses a key to customize the transformation, so that decryption can only be performed by those who know the particular key used to encrypt. In the case of DES, the block size is 64 bit, but only 56 bit are used and the remaining 8 bit can be used for parity, and then discarded in the algorithm. Therefore, the effective key length of DES is 56 bit. The algorithm's overall structure is shown in Fig. 6: there are 16 identical same processes; termed rounds. There is also an initial and final permutation, known as IP and FP (the FP is inverse function of IP (IP ―revocation‖ FP operations, and vice versa)). Before the main rounds, the block is divided into two 32 bit half block and processed at same times; this crossing process is known as the Feistel scheme. Feistel scheme is used to ensure the similarity of both the encryption and decryption processes. The only difference is the sub-key, which is reversed and used in decryption process and remaining part it is the same. This design simplifies the algorithm implementation, especially for hard implementation. The symbol denotes the (XOR) operation. The ―F- function‖ scrambles data process with one sub-key, then the output from F-function doing the XOR operation with other half block data, and the halves are swapped before the next round. After the final round, the halves are not swapped; this is a feature of the Feistel structure which makes encryption and decryption similar processes.

1.1.1 Performance Analysis-

DES (Data Encryption Standard) is a symmetric cryptographic algorithm which was adopted in January 1977 as a standard in the United States by the former National Bureau of Standards (now known as National Institute of Standards and Technology). It is widely used for protecting sensitive information's and for the authentication of banking transactions, for example. We propose here to present six different ways to break DES, the last one being currently analyzed at the LASEC.

1.1.2 Exhaustive key search

DES is an algorithm which encrypts 64 bits blocks of data using a 56 bits secret key. A common scenario is the following: we have an encrypted block at disposal, we have some information about the plaintext (we know that it is an ASCII text, or a JPEG image, for example) and we would like to recover the secret key.

The simpler method is to try to decrypt the block with all the possible keys. The information we have on the clear text will allow us to recognize the right key and to stop the search. In average, we will have to try 36'028'797'018'963'968 (36 millions of billions) of keys. Knowing that a common modern PC can check about one to two millions keys each second, this represents a work time of about 600 to 1200 years for a single machine.

1.1.2.1 A dedicated machine

An exhaustive search is quite time consuming for a single PC, but it is possible to do better. In 1998, the EFF (Electronic Frontier Foundation has built a dedicated machine in order to show to the world that DES is not (or no more) a secure algorithm. Deep Crack, that's the name of the machine, costs $200'000 and is built with 1536 dedicated chips. Deep Crack is able to recover a key with the help of an exhaustive search in 4 days in average, checking 92 billions of keys each second. Knowing the budget of electronic intelligence agencies (for example, the National Security Agency in the USA), it is easy to be pessimistic on the security of DES against such organizations!

1.1.2.2 A huge cluster of computers

One needs not even a lot of money to break DES. Volunteers who are ready to donate their machine's idle time and the Internet are sufficient. In January 1999, Distributed.Net, an organization specialized in collecting and managing computer's idle time, broke a DES key in 23 hours! More than 100'000 computers (from the slowest PC to the most powerful multiprocessors machines) have received and done a little part of the work; this allowed a rate of 250'000'000'000 keys being checked every second.

1.1.2.3 A time-memory tradeoff

An exhaustive search needs a lot of time, but negligible memory at all. It is now possible to imagine a scenario: we have a lot of available memory, and we are ready to recomputed for all the possible keys k the encrypted block y corresponding to a given block x of data and storing the pairs (y, k). So we will be able to find very quickly the right key if we have at disposal an encrypted version x' of our known block with an unknown key k' by searching in this kind of dictionary. This method becomes to be interesting in the case where we have more than one key to find and we have enough memory at disposal.In

1980, Martin Hellman proposed in a time-memory tradeoff algorithm, which needs less time than an exhaustive search and less memory than the storing method. His algorithm needs in the order of 1000 GB of storage possibilities and about 5 days of computations for a single PC.

1.1.2.4 Differential cryptanalysis

In 1990, Biham and Shamir, two Israeli cryptographers working at the Weitzmann Institute, have invented a new generic technique to break symmetric algorithms called the differential cryptanalysis. It was the first time that a method could break DES in less time than an exhaustive search. Imagine that we have a device which encrypts data with a hard-wired secret key, and imagine furthermore that we don't have the tools needed to "read" the key in the chip. What we can do is to choose some blocks of data and to encrypt them with the device. The data analysis phase computes the key by analyzing about 2^{47} chosen plaintexts. A big advantage of this attack is that its probability of success increases linearly with the number of available chosen plaintexts and can thus be conducted even with fewer chosen plaintexts. More precisely, the attack analyses about 2^{14} chosen plaintexts and succeeds with a probability of 2^{-33}.

1.1.2.5 Linear cryptanalysis

Another very important generic method to break ciphers is the linear cryptanalysis which was invented in 1994 by a japanese researcher working at Mitsubishi Electronics, Mitsuru Matsui. If we have 2^{43} = 8'796'093'022'208 known plaintext-cipher text pairs at disposal, which represents 64'000 GB of data, it is possible to recover the corresponding key in a few days using linear cryptanalysis. It is the most powerful attack on DES known at this time.A current research project at the LASEC is the cost analysis of this attack. We have first implemented a very fast DES encryption routine using advanced techniques on a common Intel Pentium III architecture; this routine is able to encrypt at a rate of 192 Mbps on a PIII 666MHz processor. We have then implemented the attack; it is currently running on 18 CPU's, breaking a DES key in 4 days.The goal of this project is to do a better statistical analysis on its complexity and on its success probability. First experimental and theoretical results have shown that a linear cryptanalysis needs in reality less time as estimated by Matsui in 1994.

1.2 International Data Encryption Algorithm

The Data Encryption Standard (DES) algorithm has been a popular secret key encryption algorithm and is used in many commercial and financial applications.Although introduced in 1976, it has proved resistant to all forms of cryptanalysis. However, its key size is too small by current standards and its entire 56 bit key space can be searched in approximately 22 hours. International Data Encryption Algorithm (IDEA) is a block cipher designed by Xuejia Lai and James L. Massey of ETH-Zürich and was first described in 1991. It is a minor revision of an earlier cipher, PES (Proposed Encryption Standard); IDEA was originally called IPES (Improved PES). IDEA was used as the symmetric cipher in early versions of the Pretty Good Privacy cryptosystem.IDEA was to develop a strong encryption algorithm, which would replace the DES procedure developed in the U.S.A. in the seventies. It is also interesting in that it entirely avoids the use of any lookup tables or S-boxes. When the famous PGP email and file encryption product was designed by Phil Zimmermann, the developers were looking for maximum security. IDEA was their first choice for data encryption based on its proven design and its great reputation.

The IDEA encryption algorithm

i. provides high level security not based on keeping the algorithm a secret, but rather upon ignorance of the secret key
ii. is fully specified and easily understood
iii. is available to everybody
iv. is suitable for use in a wide range of applications

v. can be economically implemented in electronic components (VLSI Chip)
vi. can be used efficiently
vii. may be exported world wide
viii. is patent protected to prevent fraud and piracy

1.2.1 Description of IDEA

The block cipher IDEA operates with 64-bit plaintext and cipher text blocks and is controlled by a 128-bit key. The fundamental innovation in the design of this algorithm is the use of operations from three different algebraic groups. The substitution boxes and the associated table lookups used in the block ciphers available to-date have been completely avoided. The algorithm structure has been chosen such that, with the exception that different key sub-blocks are used, the encryption process is identical to the decryption process.

1.2.2 Key Generation

The 64-bit plaintext block is partitioned into four 16-bit sub-blocks, since all the algebraic operations used in the encryption process operate on 16-bit numbers. Another process produces for each of the encryption rounds, six 16-bit key sub-blocks from the 128-bit key. Since a further four 16-bit key-sub-blocks are required for the subsequent output transformation, a total of 52 (= 8 x 6 + 4) different 16-bit sub-blocks have to be generated from the 128-bit key.

The 52 16-bit key sub-blocks which are generated from the 128-bit key are produced as follows:

i. First, the 128-bit key is partitioned into eight 16-bit sub-blocks which are then directly used as the first eight key sub-blocks.

ii. The 128-bit key is then cyclically shifted to the left by 25 positions, after which the resulting 128-bit block is again partitioned into eight 16-bit sub-blocks to be directly used as the next eight key sub-blocks.

iii. The cyclic shift procedure described above is repeated until all of the required 52 16-bit key sub-blocks have been generated.

1.2.3 Encryption

The functional representation of the encryption process is shown in Figure 1. The process consists of eight identical encryption steps (known as encryption rounds) followed by an output transformation. The structure of the first round is shown in detail. In the first encryption round, the first four 16-bit key sub-blocks are combined with two of the 16-bit plaintext blocks using addition modulo 2^{16}, and with the other two plaintext blocks using multiplication modulo 2^{16} + 1. The results are then processed further as shown in Figure 1, whereby two more 16-bit key sub-blocks enter the calculation and the third algebraic group operator, the bit-by-bit exclusive OR, is used. At the end of the first encryption round four 16-bit values are produced which are used as input to the second encryption round in a partially changed order. The process described above for round one is repeated in each of the subsequent 7 encryption rounds using different 16-bit key sub-blocks for each combination. During the subsequent output transformation, the four 16-bit values produced at the end of the 8th encryption round are combined with the last four of the 52 key sub-blocks using addition modulo 2^{16} and multiplication modulo 2^{16} + 1 to form the resulting four 16-bit ciphertext blocks.

1.2.4 Decryption

The computational process used for decryption of the ciphertext is essentially the same as that used for encryption of the plaintext. For plaintext exceeding decryption, different 16-

bit key sub-blocks are generated.More precisely, each of the 52 16-bit key sub-blocks used for decryption is the inverse of the key sub-block used during encryption in respect of the applied algebraic group operation. Additionally, the key sub-blocks must be used in the reverse order during decryption in order to reverse the encryption process. IDEA supports all modes of operation as described by NIST in its publication FIPS 81. A block cipher encrypts this fixed size, the simplest approach is to partition the plaintext into blocks of equal length and encrypt each separately. This method is named Electronic Code Book (ECB) mode. However, Electronic Code Book is not a good system to use with small block sizes (for example, smaller than 40 bits) and identical encryption modes. As ECB has disadvantages in most applications, other methods named modes have been created. They are Cipher Block Chaining (CBC), Cipher Feedback (CFB) and Output Feedback (OFB) modes.

2. LITERATURE SURVEY

Modern cryptography originates in the works of Feistel at IBM during the late 1960‘s and early 1970‘s. DES was adopted by the NIST, for encrypting unclassified information in 1977. DES is now replaced by the Advanced Encryption Standard (AES), which is a new standard adopted. Another milestone happened during 1978, marked by the publication of RSA. The RSA is the first full-fledged public-key algorithm. This discovery by and large solved the key exchange problem of cryptography. RSA also proposed the world wide acceptable standard techniques like authentication and electronic signatures in modern cryptography.

There are various issues related to DES and IDEA. Some of them are as follows

i. The 56-bit key size is the biggest defect of DES. Chips to perform one million of DES encrypt or decrypt operations a second are available (in 1993). A $1 million DES cracking machine can search the entire key space in about 7 hours.

ii. Hardware implementations of DES are very fast; DES was not designed for software and hence runs relatively slowly.

iii. Brute force is a known-plaintext attack and requires testing, on average, 2^{55} keys.

iv. Differential cryptanalysis is a chosen plaintext attack where the attacker encrypts two chosen plaintext blocks and uses the differences between the chipper text to deduce the key. This attack requires 2^{43} plaintext/cipher text pairs and $2^{55.1}$ encryption operations, making it less efficient than a brute force attack. Apparently DES was designed to be resistant to differential cryptanalysis.

2.1 Comparative study between DES and IDEA

Factors	**DES**	**IDEA**
Key length	56 bits	128 bits
Cipher Type	Symetric block cipher	Symetric block cipher
Block size	64 bits	64 bits
Cryptanalysis resistance	Vulunerable	Strong
Security	Proven inadequate	Considered Secure
Possible Keys	2^{56}	2^{128}
Time required to check all possible keys at 50 billions per second	400 days	$5*10^{23 \text{ years}}$

3. PROBLEM DOMAIN

As we have discussed in the various issues section that DES is no more secure for transmitting data over the network. It is possible to break the key of DES algorithm with present high performance systems. With 600 million instructions per second we can break the DES within 8 hours. Further if we consider that in future the speed of computer will enhance so it will be possible to break the IDEA algorithm also. So here we are proposing a new hybrid algorithm that is a combination of DES and IDEA. So this hybrid system would have combined security of both the algorithms.

4. SOLUTION DOMAIN

A Computer Network is an interconnected group of autonomous computing nodes, which use a well defined, mutually agreed set of rules and conventions known as protocols, to interact with one-another meaningfully and allow resource sharing preferably in a predictable and controllable manner. Communication has a major impact on today’s business. It is desired to communicate data with high security. With the rapid development of network technology, internet attacks are also versatile, the traditional encryption algorithms (single data encryption) is not enough for today’s information security over internet, so we propose this hybrid Cryptograph Algorithm. It is a design for transfer data with better security. At present, various types of cryptographic algorithms provide high security to information on networks, but there are also has some drawbacks. This hybrid algorithm is designed for better security by combinations of DES and IDEA.

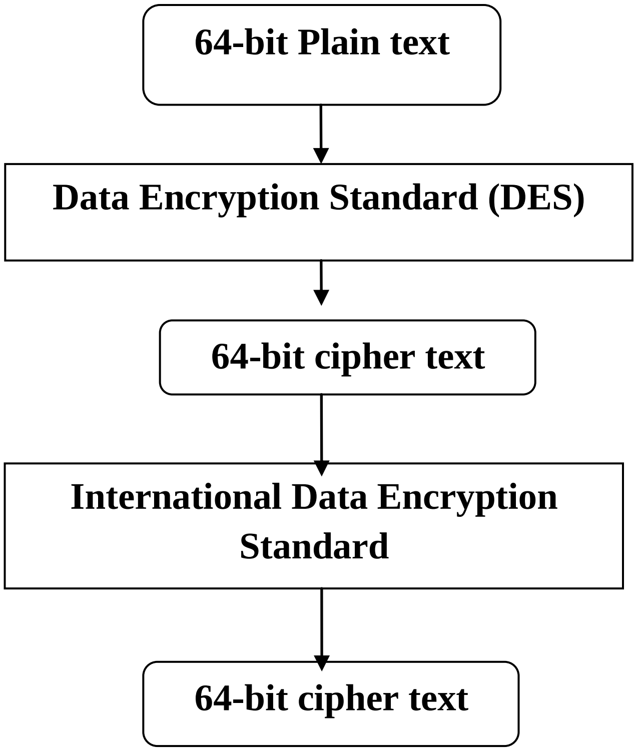
64-bit Plain text
Data Encryption Standard (DES)
64-bit cipher text
International Data Encryption Standard
64-bit cipher text

Fig. 4.1 various stages of Hybrid cryptography algorithm

4.1 Steps for Hybrid Cryptography algorithm

DES takes an input of 64-bit plaintext data block and 56-bit key (with 8 bits of parity) and outputs a 64-bit cipher text block.

1. The 8 parity bits are removed from the key by subjecting the key to its Key Permutation.
2. The plaintext and key are processed in 16 rounds consisting of:

The key is split into two 28-bit halves.

i. Each half of the key is shifted (rotated) by one or two bits, depending on the round.

ii. The halves are recombined and subject to a Compression Permutation to reduce the key from 56 bits to 48 bits. This Compressed Key is used to encrypt this round's plaintext block.

iii. The rotated key halves from step 2 are used in next round.

iv. The data block is split into two 32-bit halves.

v. One half is subject to an Expansion Permutation to increase its size to 48 bits.

vi. Output of step 6 is exclusive-OR'ed with the 48-bit compressed key from step 3.

vii. Output of step 7 is fed into an S-box, which substitutes key bits and reduces the 48-bit block back down to 32-bits.

viii. Output of step 8 is subject to a P-box to permute (scramble) the bits.

ix. The output from the P-box is exclusive-OR'ed with the other half of the data block.

x. The two data halves are swapped and become the next round's input.

3.After 16 rounds, the resultant is cipher text.

4.This resultant cipher text is a input for the IDEA

The 52 16-bit key sub-blocks which are generated from the 128-bit key are produced as follows:

i. First, the 128-bit key is partitioned into eight 16-bit sub-blocks which are then directly used as the first eight key sub-blocks.

ii. The 128-bit key is then cyclically shifted to the left by 25 positions, after which the resulting128-bit block is again partitioned into eight 16-bit sub-blocks to be directly used as the next eight key sub-blocks.

The cyclic shift procedure described above is repeated until all of the required 52 16-bit key sub-blocks have been generated.

5. SYSTEM DOMAIN

This particular algorithm can be implemented in any language like c, c++, java. Here I will implement this algorithm in java language. It needs no specific hardware and software .

1.1 Software Requirements

i. JDK (Java development kit)

1.2 Hardware Requirements

i. 128 MB RAM

ii. 8 GB Hard Disk

6. APPLICATION DOMAIN

Today, there are hundreds of security solutions available in many market areas, ranging from Financial Services, and Broadcasting to Government. IDEA is the name of a proven, secure, and universally applicable block encryption algorithm, which permits effective protection of transmitted and stored data against unauthorized access by third parties. The fundamental criteria for the development of Hybrid algorithm were highest security requirements along with easy hardware and software implementation for fast execution. This Hybrid algorithm can easily be embedded in any encryption software. Data encryption can be used to protect data transmission and storage. Typical fields are: Audio and video data for cable TV, pay TV, video conferencing, distance learning, business TV, VoIP.

There are various fields in which this Hybrid algorithm can be used. These are as follows-

i. Sensitive financial and commercial data

ii. Email via public networks

iii. Transmission links via modem, router or ATM link, GSM technology

iv. Smart cards

Encryption results in easy detection and recovery of the key. However, since there are 2^{192} possible keys, this result has no impact on the practical security of the cipher for encryption provided the encryption keys are chosen at random. IDEA is generally considered to be a very secure cipher and both the cipher development and its theoretical basis have been openly and widely discussed so this Hybrid algorithm will result into higher security. IDEA is a patented and universally applicable block encryption algorithm, which permits the effective protection of transmitted and stored data against unauthorized access by third parties. With a key of 128 bits in length, IDEA is far more secure than the widely known DES based on a 56-bit key. The fundamental criteria for the development of IDEA were military strength for all security requirements and easy hardware and software implementation. The algorithm is used worldwide in various banking and industry applications. They predestine the algorithm for use in a great number of commercial applications.

7. EXPECTED OUTCOME

This hybrid algorithm has high security of data transmission over the network. This whole work is focused on how we can increase the security of data transmission. Security is necessary when we transmit highly sensitive data such as Banking transactions, Military information and many more.This hybrid algorithm fulfills these criteria up to the mark. This work results into more secure transmission of data comparatively DES, IDEA and AES data encryption algorithms.

8. FUTURE SCOPE

This proposed hybrid algorithm can be made much more powerful and secure by increasing the number of iterations in the encryption algorithm to suit the level of security required. An inverse policy of reducing the number of iterations for lower security can also be employed. We can also go for combining another algorithm that will encrypt data given by the IDEA algorithm. This inclusion of third algorithm will increase the security but there are two phase of a coin. As a result Security will increase but time that is taken to convert the plain text into final cipher text will be greater than previous hybrid algorithm. So it is the demand of application in which you are going to use security algorithm which factor is important time or security. We must play a fair role between time taken by the algorithm and level of security, both must be reasonable.

References

[1] Sombir Singh, Sunil k. Maakar, Dr. Sudesh Kumar "Enhancing the Security of DES Algorithm Using Transposition Cryptography Techniques",IJARCSSE, Volume 3, Issue 6, pp 464-470, June 2013.

[2] Nick Hoffman "A Simplified IDEA Algorithm" Department of Mathematics, Northern Kentucky University pp 1-5, 2007.

[3] Meier, W., On the Security of the IDEA block cipher, Advances in Cryptology.

[4] Atul Kahate "Cryptography and Network Security" second edition

[5] Shaaban Sahmoud, Wisam Elmasry and Shadi Abdulfa "Enhancement the security of AES againt modern attacks by using variable key block cipher",

International Arab journal of e-technology, vol. 3, No. 1, January 2013

[6] Vishwa Gupta, Gajendra singh, Ravindra Gupta " Advance cryptography algorithm for improving data security", IJARCSSE Volume 2, Issue 1, January 2012

[7] Data Encryption Standard (DES), Federal Information processing standards, Publication 46-3, 1999 October 25

[8] Advanced Encryption Standard, National Institute of Standards and Technology (US), URL:http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

[9] William Stallings:"Cryptography and network security:Principles and Practices".

[10] Advanced Encryption Standard, [online], Available: URL:http://en.wikip/Advanced_Encryption_Standard

[11] Wang Tianfu, K. Ramesh Babu "Design Of A Hybrid Cryptographic Algorithm IJCSCN vol 2(2),277-283