International Journal of Current Engineering and Technology
E-ISSN 2277 – 4106, P-ISSN 2347 – 5161
Available at http://inpressco.com/category/ijcet

Research Article

Relative Performance-based Study of Data Encryption Standards

Mahak*

Department of CSE, Kurukshetra University Kurukshetra, India

Accepted 16 June 2016, Available online 30 June 2016, **Vol.6, No.3 (June 2016)**

Abstract

The principal goal leading the design of any encryption algorithm must be security against unauthorized attacks. An Algorithm is considered computationally secure if it cannot be fragmented with standard resources, either current or future. For any encryption algorithm, performance and the implementation's cost must be considered before its realization. Other important issues to be considered in performance evaluation of encryption standards are its execution time, memory requirements and hardware or software needs. A data encryption algorithm would not be of much use if it is secure enough but slow in performance as some real-world applications of encryption algorithms include e-banking, online purchasing, share market and online transaction processing applications. In this paper, the four of the popular secret key encryption standards, i.e., DES, 3DES, AES, IDEA and a new encryption approach BEST have been implemented, and their performance is compared by encrypting input files of varying texts and sizes. Based on all experiments, it is concluded that BEST algorithm proves the most optimal encryption standard for textual data.

Keywords: *AES, BEST, Cryptography algorithms, DES, Decryption, Encryption, IDEA, Triple-DES.*

1. Introduction

There are a lot of security approaches that can be applied to keep the data secure while transmitting. The most premium technique used for secure transfer of data is Cryptography. It is defined as the technique of converting data from plain format into ambiguous and unintelligent format, so that eavesdroppers do not have any clue about type and content of data being transferred(P.P Charles *et al,*2008) Cryptography can be classified into two disciplines: Block and Stream Cipher, according to the number of bytes encrypted at a single pass. Out of these two techniques, Block Cipher is most widely adapted technique because of its speed and performance advantage over stream cipher. It picks up blocks of data and encrypts it in one pass, hence achieving faster execution of encryption (William Stalling, 2007). In this paper, the security and performance of the principal block ciphers has been compared. While comparing the performance of algorithms, the execution time, memory requirements and security issues are measured.

To make sure that all encryption standards have a fair chance, they are implemented in one standard language i.e Java. Java has been implemented here because of its advanced features like platform independence and support for Unicode.

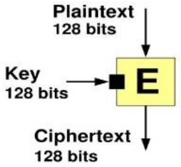


Figure 1: Working of a Block Cipher

2. Encryption Algorithms

The following secret key encryption algorithms were opted for comparison:

- DES
- Triple-DES
- AES (Rijndael)
- IDEA
- BEST

A. Data Encryption Standard (DES)

DES is based on a symmetric-key encryption concept which uses a 56-bit key and is most extensively used in the world. It is a block cipher that was selected by the National Bureau of Standards as an official encryption standard for the United States in 1976. It works on 64-bit data by using Feistel function i.e. dividing 64-bit data into 2 blocks of 32-bit and implementing binary XOR on it for 16 rounds (L.Brown *et al,*1990)(P.P Charles *et al,*2008) The Feistel function ensures that encryption and decryption are similar processes. DES

*Corresponding author is a PhD Scholar

faced a lot of criticism due to short key length but despite of all disputes, DES was selected as a standard in encryption algorithms. It was widely used in banking industry and was gain international recognition for many years. By late 1990s, DES faced defamed when in January 1999, distributed.net and the Electronic Frontier Foundation collaborated to publicly break a DES key in 22 hours and 15 minutes (E.Biham etal,1991). Speed of DES also became a concern and that's the reason why Triple-DES was invented.

B. Triple-DES (3DES)

Triple-DES is the common name for the Triple Data Encryption Algorithm (TDEA). The triple-DES algorithm was needed as a replacement for DES due to advances in key searching. 3DES is a proposal based on the existing DES, and was standardized in ANSI X9.17 & ISO 8732 and in PEM for key management. Triple DES uses a key bundle which comprises three DES keys, K_1, K_2 and K_3, each of 56 bits[10]. The encryption algorithm is:

ciphertext = $E_{K3}(D_{K2}(E_{K1}(\text{plaintext})))$

i.e., DES encrypts with K_1, DES *decrypt* with K_2, then DES encrypt with K_3. Decryption is the reverse:

plaintext = $D_{K1}(E_{K2}(D_{K3}(\text{ciphertext})))$

i.e., decrypt with K_3, *encrypt* with K_2, then decrypt with K_1.

3DES works on 64-bit block of data like DES. In 3DES, following key options are possible:

- All three keys are independent.
- K_1 and K_2 are independent, and $K_3 = K_1$.
- All three keys are identical, i.e. $K_1 = K_2 = K_3$.

Keying option 1 is the strongest, with 3 x 56 = 168 independent key bits. Keying option 2 provides less security, with 2 x 56 = 112 key bits. This option is stronger than simply DES encrypting twice, e.g. with K_1 and K_2, because it protects against man-in-middle attacks. Keying option 3 is no better than DES, with only 56 key bits. This option provides backward compatibility with DES (as K1=K2=K3), because the first and second DES operations simply cancel out. 3DES can work in different modes for different blocks of data. The best attack known on keying option 1 requires around 2^{32} known plaintexts, 2^{113} steps, 2^{90} single DES encryptions, and 2^{88} memory. If the attacker seeks to discover any one of many cryptographic keys, there is a memory-efficient attack which will discover one of 2^{28} keys, given a handful of chosen plaintexts per key and around 2^{84} encryption operations (E.Biham *et al,*1991)

C. Advanced Encryption Standard (AES)

In September 1997, US NIST announced a call for candidate ciphers for its new Advanced Encryption Standard, because clearly a replacement for DES was needed at that time.

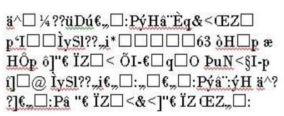
Cryptographic algorithms were called in 1998 and 5 were short-listed in August 99. Finally, Rijndael was selected as the AES finalist in October 2000. The Rijndael cipher was developed by two Belgian cryptographers, Joan Daemen and Vincent Rijmen, and submitted by them to the AES selection process(J.Deamen etal). The standard comprises three block ciphers: AES-128, AES-192 and AES-256. The AES candidates are the latest generation of block ciphers, and have a significant increase in the block size - from the old standard of 64-bits up to 128-bits; and keys from 128 to 256-bits.The Best public cryptanalyst related-key attack can break 256-bit AES with a complexity of $2^{99.5}$,which is faster than brute force attack. The only successful published attacks(B.Schneier etal,1998) against the full AES were side-channel attacks on some specific implementations till May 2009.

D. International Data Encryption Algorithm (IDEA)

International Data Encryption Algorithm (IDEA) is a block cipher designed by James Massey of ETH Zurich and Xuejia Lai that was first described in 1991. It was designed in a way to replace DES as encryption standard. It works on symmetric-key encryption, hence encoding and decoding are exactly reverse processes in respect to each other. IDEA is a minor revision of an earlier cipher, PES (Proposed Encryption Standard); IDEA was originally called IPES (Improved PES). Today IDEA is a licensed cryptosystem in most of the countries and is available free of cost to anyone. It uses a 128-bit key and works on block of 64-bit data. Each round uses six 16-bit sub-keys, while the half-round uses four, a total of 52 for 8.5 rounds(Herbert). The first eight sub-keys are extracted directly from the key, with K1 from the first round being the lower sixteen bits; further groups of eight keys are created by rotating the main key left 25 bits between each group of eight. This means that it is rotated less than once per round, on average, for a total of six rotations. One round of IDEA consists of series of eight identical transformations and an output transformation. IDEA does a lot of bitwise binary operations like XOR, addition modulo 2^{16}, etc on the plaintext. IDEA is considered one of the most secure cryptographic algorithms implemented so far. The best attack against IDEA could break its keys till round 6 out of 8.5 rounds, assuming non-input of weak keys (i.e. keys with more number of zeros). However, now there are faster and securer algorithms which stand more chance in hard cryptanalysis.

3. Performance Results

To make a fair comparison between security and performance check of above mentioned algorithms, each is implemented using Java language. The reason behind choosing Java language is its support to Unicode; it makes these algorithms adaptive to any natural language across the globe. The basic feature of popular block ciphers is that they all are fully dependent on key and the key remains same for the whole plaintext[9]. This produces same cipher text every time a key is applied on the plaintext. This is a major disadvantage of block ciphers. DES, 3DES, AES and IDEA suffer from the above mentioned drawback of block ciphers, but BEST algorithm has been designed to overcome this hitch.



ä^□ ¼??üDú€„□:PýHâ¨Èq&<ŒZ□
p‘I□□ÌySl??„i*□□□□□63 òH□p æ
HÔp ô]"€ ÏZ□< ÕI-€□q□O ÞuN<§I-p
î]□@ ÌySl??„i€„□:„□€„□:Pýâ¨:ýH ä^?
?]€„□:Pâ "€ ÏZ□<&<]"€ ÏZ ŒZ„□:

Figure 2: Ciphertext obtained after BEST encryption

BEST algorithm keeps changing the key based on randomly selected integer number and sequence symbol. This feature makes BEST algorithm immune to the Replay attacks (E.Biham etal,1991), making it computationally more secure. In addition, it does different binary operations on plaintext or prior cipher text making it harder to crack than established block ciphers.

A. Estimation of Execution Times

For obtaining accurate and repeatable execution time measurements, all experiments have been executed on Core-2-duo processor, 2.4 GHz machine running Microsoft Windows XP operating system. The basic plus point of any encryption algorithm is the speed of encoding and decoding processes. Please note that the larger the block size, the faster the algorithm will be. The following tables show encryption and decryption times of cryptosystems being compared:

Table 1. Comparative performance analysis of encryption times

Input Size (Bytes)	DES	3DES	AES	IDEA	BEST
20527	2	7	4	1.73	0.44
36002	4	13	6	3.03	0.7
45911	5	17	8	3.87	1
59862	7	23	11	5.05	1.3
69646	9	26	13	5.87	1.51

Table 2. Comparative performance analysis of decryption times

Input Size (Bytes)	DES	3DES	AES	IDEA	BEST
20527	17	58	62	9.87	0.35
36002	30	99	94	17.3	0.62
45911	41	130	125	22.08	0.8
59862	52	181	174	28.79	1.04
69646	69	201	200	33.5	1.21

As evident from the above tables, the total execution time of BEST (sum of encryption and decryption times) is much lesser than other conventional encryption standards. The ranking of encryption standards on the basis of their execution time (in decreasing order of execution time) is as follows:

1. BEST
2. IDEA
3. DES
4. AES
5. Triple DES

Table 3. Comparative performance analysis of execution times

Input Size (Bytes)	DES	3DES	AES	IDEA	BEST
20527	19	65	66	11.6	0.79
36002	34	112	100	20.33	1.32
45911	46	147	133	25.95	1.80
59862	59	204	185	33.84	2.34
69646	78	227	213	39.37	2.72

A. Memory Requirements

Memory requisites of encryption algorithm takes into account: the size variation of plaintext versus ciphertext and key management issues like key length of algorithm.

Table 4. Comparitive memory requirements

Encryption Algorithms	Key Length (Bits)	Plaintext Size (Bits)	Cipher Text (Bits)
DES	56	64	64
3DES	168	64	64
AES	128	128	128
IDEA	128	64	64
BEST	24	32	32

The above table shows that memory requisites of BEST algorithm is better than other encryption standards; it is almost one-fourth of AES.

C. Security Analysis

The main basis of comparison of encryption algorithms is the trade-off between security and performance. A cryptanalysis study reveals that performance of algorithms should be measured by number of rounds for each algorithm to check its security against brute-force attack. A large number of rounds make the algorithm slower but are supposed to provide greater security. However, it cannot be exactly true as it also depends upon the binary operations and additional mechanisms adopted by a cryptographic algorithm. In practice, most failures in cryptographic systems derive not from weaknesses in the algorithms used but rather from the exploitation of subtle flaws in the way the algorithms are implemented or through the exploitation of interactions between algorithm implementations and the environments in which they operate. All above mentioned security algorithms are broken except BEST algorithm. BEST algorithm is basically a partial-symmetric key encryption technique i.e. it doesn't depend fully on the secret key, rather it also uses a secondary key for further protection against eavesdroppers. According to cryptanalysis of BEST, following results are achieved:

E. Block Encryption Standard for Transfer of Data (BEST)

This new proposed BEST algorithm is a block cipher that divides data into blocks of equal length and then encrypts each block using a special mathematical set of functions known as key. This algorithm uses a partial-symmetric key approach for encoding and decoding of data i.e. it do not depend entirely on the secret key for encryption(A.kaushik *et al* 2010). It uses ASCII code to handle famous natural languages like English, Spanish, etc. Here, two predefined stacks along with a logic based lookup concept are taken. The first stack holds some specially chosen symbols, where other stack contains a random number from a preselected range by a predefined method to make the code sequence more secure. The encryption process does a variety of binary operations like Shift Left Operation on the message for protecting it against unauthorized attacks. Additional security measures are used in algorithm to change the format of key while sending it from one end to another. Thus, the key distribution predicament can be handled easily. Another plus point of BEST algorithm is that it protects the cipher text from Brute-force attacks as the key is changed many times in the encryption process. Thus even knowing or decrypting one key, it will be very hard to attain plaintext from cipher text.

1) Possible number of attempts to break primary encryption key is $2^{10}*2^{24}$ units of time.
2) Possible number of attempts to break secondary encryption key is 2^{32} units of time.

Hence, it can be explored that BEST algorithm stands out more securer than other standard algorithms.

Conclusion

In this paper, the popular secret key algorithms including DES, 3DES, AES, IDEA and BEST were implemented, and their performance was compared by encrypting input files of varying contents and sizes. The algorithms were implemented in a uniform language, using their standard specifications, and were tested on different file sizes, to compare their performance. In the end, the results were presented which conclude that the BEST is the fastest algorithm with low memory requirements. However, the security analysis also suggests that BEST algorithm provides best security against any unauthorized attacks as compared to any other encryption standard.

References

A. Kaushik, M. Barnela ;. Kumar (2010), Block Encryption Standard for Transfer of Data (BEST), M anila, Philippines.

B. Schneier; J. Kelsey;D. Whiting; D. Wagner, C. Hall, ; N. Ferguson (1998), Performance Comparison of the AES Submissions, Counterpane Systems. http://www.counterpane.com/AESperformance.html

E. Biham ; A. Shami (1991)r, Differential Cryptanalysis of DES-like Cryptosystems, *Journal of cryptology* , Vol. 4, No. 1

Daemen ; V. Rijmen, The Block Cipher Rijndae l, Cardis.

L. Brown ; J. Seberry(1990) Key scheduling in DES type Cryptosystems.

Ma Yide, *et al* (2005), Some Improvements on Internati onal Data Encryption Algorithm in Developing System, *Computer Engineering and Applications,* Vol.41, Issue 7,pp. 114-115.

National Institute of Standards and Technology, Specification for the Advanced Encryption Standard (AES). FIPS PUB 197, available at http://csrc.nist.gov

P.P Charles ; P.L Shari (2008) *Security in Computing:* 4th edition, Prentice-Hall, Inc., pp 40-42.

S. Hebert, A Brief History of Cryptography, an article available at http://cybercrimes.net/aindex.html.

W.Stallings(2007) Cryptography and network security principles practice, Fourth edition, Prentice hall.