УДК 004.056.55
МРНТИ 81.93.29

COMPARATIVE STUDY OF SYMMETRIC CRYPTOGRAPHIC ALGORITHMS

A.N. NURGALIYEV

International Information Technology University

Abstract: *This article represents an equitable comparison between the most popular and frequently used algorithms in the data encryption area. There are some main characteristics that distinguish encryption algorithms: elapsed time and efficiency of data encryption and ability to protect data from various attacks. This document presents the comparison between the most common symmetric encryption algorithms: DES, 3DES, Blowfish, and AES. The comparison was done by processing data blocks of different sizes to estimate the encryption and decryption speed. Since our main task is to perform these algorithms with different settings, the presented comparison takes into account the behavior and performance of the algorithm when using different data loads. This paper also analyzes parameters such as flexibility, key extension option, possible attacks and security vulnerability of the algorithms, which determines the efficiency of the cryptosystem.*

Keywords: *Encryption Algorithms, Cryptography, AES, DES, Blowfish, TripleDES*

ШИФРЛАУДЫҢ СИММЕТРИЯЛЫҚ АЛГОРИТМДЕРІН САЛЫСТЫРМАЛЫ ТАЛДАУ

Аңдатпа: *Бұл мақала деректерді шифрлау саласында ең танымал және жиі қолданылатын алгоритмдерді объективті салыстыру болып табылады. Шифрлау алгоритмдерін ерекшелейтін бірнеше негізгі сипаттамалар бар: кеткен уақыт, деректерді шифрлау тиімділігі және деректерді әртүрлі шабуылдардан қорғау қабілеті. Бұл құжатта des, 3DES, Blowfish және AES симметриялық шифрлаудың ең көп таралған алгоритмдері арасындағы салыстыру ұсынылған.*
Салыстыру шифрлау және дешифрлау жылдамдығын бағалау үшін әртүрлі өлшемдегі деректер блоктарын өңдеу арқылы жасалды. Әрқилы параметрлермен осы алгоритмдерді орындау біздің басты міндетіміз болғандықтан, ұсынылған салыстыру сан түрлі деректер жүктемелерін пайдалану кезінде алгоритмнің мінез-құлқы мен өнімділігін ескереді. Бұл мақалада криптожүйенің тиімділігін анықтайтын икемділік, кілтті кеңейту мүмкіндігі, ықтимал шабуылдар және алгоритмдердің осалдығы сияқты параметрлер талданады.

Түйінді сөздер: *Шифрлау алгоритмдері, криптография, AES, DES, Blowfish, Triple DES*

СРАВНИТЕЛЬНЫЙ АНАЛИЗ СИММЕТРИЧНЫХ АЛГОРИТМОВ ШИФРОВАНИЯ

Аннотация: *Данная статья представляет собой объективное сравнение наиболее популярных и часто используемых алгоритмов в области шифрования данных. Существует несколько основных характеристик, которые отличают алгоритмы шифрования: затраченное время, эффективность шифрования данных и способность защищать данные от различных атак. В этом документе представлено сравнение между наиболее распространенными алгоритмами симметричного шифрования: DES, 3DES, Blowfish и AES. Сравнение было сделано путем обработки блоков данных разных размеров для оценки скорости шифрования и дешифрования. Поскольку нашей главной задачей является выполнение этих алгоритмов с различными настройками, представленное сравнение учитывает поведение и производительность алгоритма при использовании различных нагрузок данных. В этой статье также анализируются такие параметры как гибкость, возможность расширения ключа, возможные атаки и уязвимость алгоритмов, которая определяет эффективность криптосистемы.*

Ключевые слова: *алгоритмы шифрования, криптография, AES, DES, Blowfish, TripleDES*

Introduction

Cryptography, it is the process of keeping and transferring data in a special form that only the authorized participants can interpret. The operation of transformation information into a secret, encrypted code for transmission through a public network. Nowadays, most of the cryptography processes are digital, where the original text (also called as "plaintext") is turned into a encrypted equivalent which called "ciphertext" by different encryption algorithms. The ciphertext is decrypted at the receiving side and returns into plaintext and for secured and safe data communications. This is a technique, which is used to avoid unauthorized access of data. The encryption process consists of single or multiple keys to hide the data from the intruders and imposters.

The cryptography methods are classified on the basis of their key selection. The section shows the advantages of various cryptographic techniques.

Symmetric (Private) Cryptography.

Symmetric (also known as a private-key encryption) involves using the same key for encryption and decryption processes. Encryption includes applying an operation (an algorithm) to the data to be encrypted using the private key to make them unintelligible. Even the weakest algorithm (for example an exclusive OR) could make the system nearly tamper proof. Users have the provision to update the keys and use them to receive the subkeys. It is much effective and fast approach as compared to asymmetric key cryptography. In symmetric key cryptography key has been generated by the encryption algorithm and then send it to the receiver section and decryption takes place [1].

Asymmetric (Public) Cryptography.

Asymmetric cryptography is the type of cryptography in which a pair of keys is used to encrypt and decrypt the data. First of all, a network user requests a public and private key pair. A user who wants to send an encrypted data can get the intended recipient's public key from a public administrator. The method is more secure instead of private key cryptography but it consumes more power and more processing time. Due to increase in the computational unit the overheads are high in public key cryptography [1].

Modern Cryptography.

A combination of both public and private key cryptography is known as modern cryptography. A pair of public and private keys has been used to encrypt and decrypt the data. The technique has the salient features of private key: fast speed, easy to process and features of public key such as secured, avoid key transportation, provide the power to the users to generate their own keys of variable length. Users also have the possibility to upgrade the key at any time. In this technique certification authority has been used to keep the track of the entire system and keys [5].

The generation, modification and transportation of keys have been done by the encryption algorithm. It is also known as cryptographic algorithm. There are a big amount of cryptographic algorithms are available to encrypt the data. Their strengths depend on the cryptographic system. Any computer system, which involves cryptography is known as cryptographic system, the strength of encryption algorithm heavily relays on the computer system, which is used for the generation of keys. The computer systems take the responsibilities sending the secret information over the web with the help of cryptographic hash functions, key management and digital signatures. Crypto systems are composed from cryptographic primitives such as encryption algorithm, number of keys, hash and round functions, memory elements, real time operating system, etc.

Types of encryption algorithms

- Data Encryption Standard (DES).

It is one of the most widely accepted, publicly available cryptographic systems today. It was developed by IBM in the 1970s but was later adopted by the US government as a national bureau of standards as an official Federal Information Processing Standard (FIPS)

for the United States in 1976. It uses a 56-bit key to encrypt the 64 bit block size data. It processes 64-bit inputs into 64-bit cipher-text and algorithm performs 16 iterations [2].

- Triple Data Encryption algorithm (3DES)

3DES is originated from DES and in its encryption uses 3 different keys of 56 bits, in sum 168 bits [2]. There are three key options:

First, each of keys are independent. This option is the most secure and strongest using 168 independent key bits.

The second option involves when all keys are identical and this is the weakest feature because 3DES encryption algorithm turns into DES algorithm.

The last option is to convert the first two options: the third and the first keys are identical. It executes 48 rounds of processing to encrypt the data using DES algorithm three times. 3DES increases the security level of DES combining key size of 168 bits (56 bits 3 times) what is beyond the reach of brute force methods. 3DES algorithm has been estimated suspicious as a consequence of DES issues but in fact there is no any serious vulnerabilities. Nowadays a large number of Internet protocols are using this cryptosystem. 3DES is vulnerable in some variations of meet-in-the-middle attack (MITM). It also undergoes differential attacks and related-key attacks [5].

- Advanced Encryption Standard (AES).

It is a symmetric 128-bitblock data encryption technique developed by Belgian cryptographers Joan Daemen and Vincent Rijmen. The U.S government adopted the algorithm as its encryption technique in October 2000, replacing the DES encryption it used. AES works at multiple network layers simultaneously. The National Institute of Standards and Technology (NIST) of the U.S. Department of Commerce selected the algorithm, called Rijndael (pronounced Rhine Dahl or Rain Doll), out of a group of five algorithms under consideration, including one called MARS from a large research team at IBM. While the terms AES and Rijndael are used interchangeably, there are some differences between the two. AES has a fixed block size of 128-bits and a key size of 128, 192, or 256-bits, whereas Rijndael can be specified with any key and block sizes in a multiple of 32-bits, with a minimum of 128-bits and a maximum of 256-bits [3].

- BLOWFISH

Blowfish is a 64-bit block cipher with a variable-length key. The algorithm consists of two parts: key expansion and data encryption/ decryption. Extension of the key converts a key of up to 448 bits into several arrays of subkeys, with an overall size of 4168 bytes.[4]

Information encryption consists of a simple function, consequently performed 16 times. Every step consists of a key-dependent permutation and a key-dependent and dependent on a substitution of data. Only the addition and exclusive or of 32-bit words are used. At each step the only additional operations are four data extractions from the indexed array. Blowfish uses a lot of subkeys. These subkeys must be calculated before encryption or information decryption begins.

The P-array consists of 18 32-bit subkeys:

P1, P2, . . ., P18

Every of the four 32-bit S-boxes contains 256 elements:

S1,0, S1,1, . . ., S1,255

S2,0, S2,2, . . ., S2,255

S3,0, S3,3, . . ., S3,255

S4,0, S4,4, . . ., S4,255

The exact method used to calculate these subkeys is described in this section below (Fig.1).

Blowfish is a Feistel network consisting of 16 phases. A 64-bit x data element is input. For encryption:

Divide x into two 32-bit halves: xL, xR

For i = 1 to 16:

$xL = xL \oplus P18$

$xR = F(xL) \oplus xR$

Rearrange xL and xR (except for the last phase)

$xR = xR \oplus P17$

$xL = xL \oplus P18$

Combine xL and xR

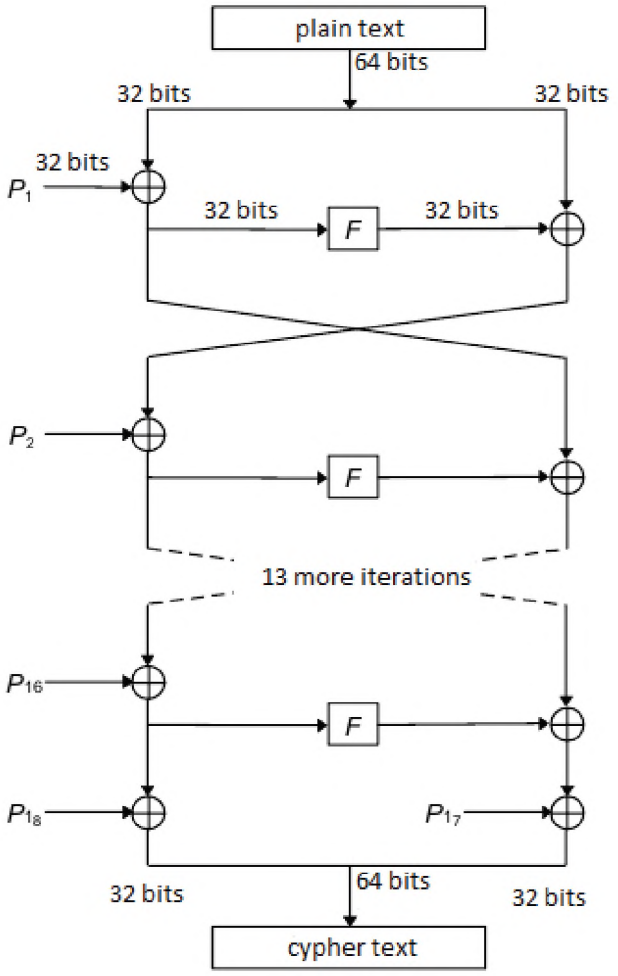

Figure 1 – Blowfish algorithms scheme

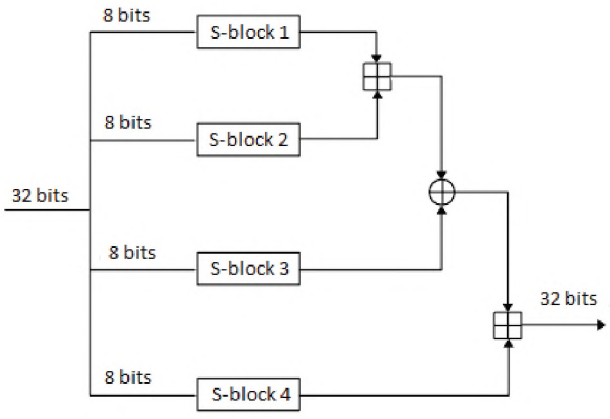

Figure 2 – F function

The function F (Fig.2) is as follows:
xL division into four 8-bit parts: a, b, c, and d.
F(xL) = ((S1,a + S2,b mod 2^32) ⊕ S3,c) + S4,d mod 2^32.

The decryption is the same as encryption, but P1, P2,. . ., P18 are used in inverse order.

Comparison of cryptographic algorithms based on various parameters.

Among the large number of existing cryptographic algorithms, DES, 3DES, BLOWFISH, AES are selected and compared on the basis of used structure, ability to expand, security and crypto-resistance. [2]. Table 1 shows the comparative study on selected encryption algorithms.

Table 1 – comparative study of symmetric encryption algorithms

Algorithm	Structure	Flexibility and Modification	Known Attacks
DES	Feistel network	Unmodified	Brute-Force Attack
3DES	Feistel network	Could be extended from 56 up to 168 bits	Brute Force Attack, Chosen Plaintext, Known Plaintext
AES	Substitution-Permutation	Could be modified with a condition: 256 key length in multiples of 64	Side Channel Attack
BLOWFISH	Feistel network	Could be modified with a condition: 64-448 key length in multiples of 32	Dictionary Attack

Security of encryption algorithms is based on how resistant the algorithm against various attacks. The execution of these encryption algorithms is based on number of aspects: key length, block size, structure, cryptographic time and number of rounds used. Eventually, these factors directly affects the security of a particular algorithm. The size of blocks plays a vital role in encryption and decryption processes, which is the basic unit of data.

Larger block size provides higher security whereas other factors were estimated to be almost equal in some algorithms. AES algorithm uses block size of 128 bits which is twice bigger than other selected symmetric algorithms. Next critical evaluation is the number of rounds used for encryption/decryption process (see Figure 3).

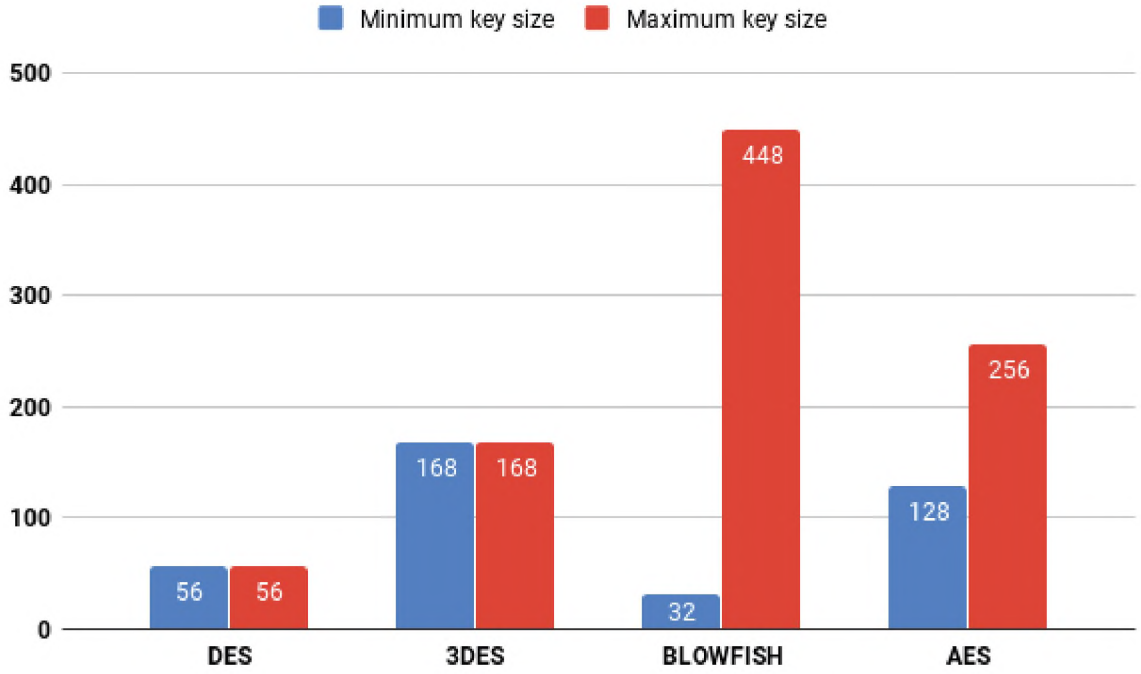

Figure 3 - Quantitative measures – Key Size (Bits)

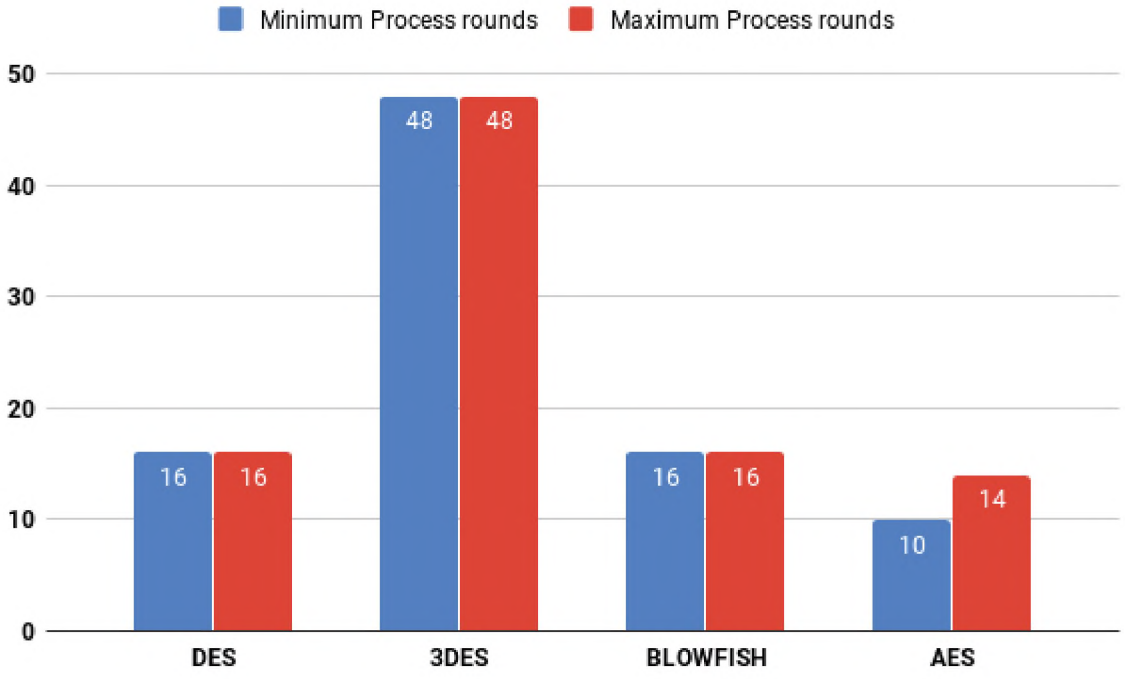

Figure 4: Quantitative measures – Key Size (Bits)

Increase in processing rounds strengthens the security because single Feistel round provides insufficient security. DES and BLOWFISH has 16 rounds of encryption process. 3DES has 3 times of DES what means it has 48 rounds. AES has varying number of rounds which is depending of key size. The major issue with symmetric key algorithms is a brute force attack, where all possible keys are tried until the exact key is found to decrypt the message. Longer key lengths reduce the feasibility of attacks, since the number of key combinations increase (see Figure 4).

DES has a weak key of 56 bits. 3DES has 168 bits key with good resistance against attack. AES has variable key lengths of 128, 192, and 256 which provide a larger number of key combinations. BLOWFISH uses 448 bit keys which are considered to be longest and strongest as far as brute force attacks are concerned. Security of the cryptosystem is defined by a secured encryption scheme to guard against brute force attacks and differential plaintext-cyphertext attack. Though DES and 3DES are faster but they are less secure due to weak keys. The analysis shows in case of symmetric algorithms Blowfish and AES that they are considered to be secure and efficient based on high security and less limitations. Another criteria is the expansion and flexibility of Blowfish and AES which is high compared to other symmetric algorithm.

Conclusion

This paper provides an analytical study on various symmetric encryption algorithms such as DES, 3DES, BLOWFISH, AES. The analysis is based on the structure of the algorithms, the security aspects and the limitations they have. AES and DES algorithms showed poor crypto resistance, while Blowfish and 3DES have not any known security weak points.

REFERENCES

1. G. Abood, O. and K. Guirguis, S. (2018). A Survey on Cryptography Algorithms. *International Journal of Scientific and Research Publications*.
2. Nadeem, A. and Dr. Javed, Y. (2005). A Performance Comparison of Data Encryption Algorithms.
3. National Institute of Standards and Technology. and National Institute of Standards and Technology. (2001). *F.I.P. Standard, Advanced Encryption Standard (AES),*. pp.13-27.
4. Schneier, B. (n.d.). *Schneier on Security: The Blowfish Encryption Algorithm*. [online] Schneier. com. Available at: https://www.schneier.com/academic/blowfish/
5. Schneier, B. (1996). *Applied Cryptography*. John Wiley & Sons.