A Comprehensive Comparison of Symmetric Cryptographic Algorithms by Using Multiple Types of Parameters

Muhammad Usman[1], Ijaz Ali Shoukat[2], Muhammad Sheraz Arshad Malik[3], Mahwish Abid[4], Muhammad Mashhood ul Hasan[5], Zainab Khalid[6]

Department of Computer Science, Riphah International University Faisalabad Campus, Pakistan[1,2,4,5,6]
Department of Information Technology, Government College University Faisalabad, Pakistan[3]

Abstract

In modern world the use of internet is increasingly rapidly and data exchanged over internet is increasing on daily basis. More the data or transactions carried out over internet more there's a need to secure data. Security is a main concern as they play with confidentiality of data either in every field. Cryptography is one of the best option to overcome this as it maintain the privacy of user and this cannot be implemented with use of encryption process. There are two types of cryptographic techniques namely symmetric and asymmetric. In this study a comprehensive comparison among multiple symmetric techniques is discussed in detail.

Key-terms:

Symmetric Ciphers, Block Cipher, IOT, dynamic nature, Modern Ciphers, security metric.

1. Introduction

One of the top priorities of state is to acquire appropriate countermeasures to protect its national information. Main reason for this tendency is to improve performance & security of communication system for a country. Easy and fast accesses to information comprising computing resources are sharing the internet and these may be considered as requirement of developed country. Information Technology is becoming popular now-a-days and information security hence is considered as basic component. Requirement of information security has been increased because of access use of internet, distributed network and communication facilities. Efficiency and operation of information system application depends on their security and reliability.

Security is the most challenging aspects over the internet and in network applications. Ratio of the exchanged data over the internet is increasing rapidly. Cryptography is the modern science of achieving security by encoding messages in unreadable format and original message can only be readable from only intended user. The main goal of cryptography is to keep the data privacy from unauthorized access[1][2]. It is the practice to provide secure communication in presence of adversaries to maintain information security such as data confidentiality, data integrity, authentication, and non-repudiation. The process to convert plain text into unintelligible text or cipher text in cryptography is called encryption. The cipher text is understandable only to someone who knows how to decrypt it. Message or information is encrypted using an encryption algorithm. Usually this is done with the use of an encryption key, which specifies how the message is to be encoded. Any intruder that can see the cipher text should not be able to analyze the original message[3].

Data owner is able to decipher the text using a decryption algorithm which usually requires a secret decryption key. There are many of cryptographic algorithms used for encrypting data and most of all fall into two general categories Public key system and Private Key system. Public key system is known as asymmetric algorithm and private key system are known as symmetric algorithms. Symmetric and asymmetric are widely accepted types of cryptography in which symmetric is focused towards ensuring secure communication between sender and receiver by using same key at both ends, and asymmetric requires one key for encryption and second for decryption[2]. In this research paper different symmetric cryptographic algorithms are analyzed and a comparative study is discussed while considering multiple parameters.

2. Literature Review

2.1 Background Concepts: Symmetric Ciphers

It is already known that use of internet and online transaction is increasing every second at high rate and demand of securing terabytes of data present over the internet is challenge. Term 'Cryptography' is essential part of information security making the virtual humanity a safer place. There are many cryptographic algorithms present that can be used. Data owner prefers cryptographic algorithm which has low cost and high performance. However, in actual those algorithms which are one stop door to solution does not exist. At present there are many

Manuscript received December 5, 2018
Manuscript revised December 20, 2018

common algorithms with an outlay of performance trade off [4][5].

2.2 Symmetric Encryption Algorithms

- **DES:**

DES originated in 1970's when US government's needs security for their data and sensitive information. NIST petitioned proposal but none of the proposals were suitable. In 1974, IBM came up with algorithm based on HosrtFiestal namely Lucifier Cipher which was accepted by during 1973-1974[6].

Data encryption standard (DES) was considered as symmetric block cipher used for encryption of data. It was derived from IBM proposed algorithm called lucifier[7]. DES was designed in 1970's by IBM and later in 1975's adopted by NIST as Federal Information Processing Standard (FIPS). It takes fixed length of plaintext and by transforming through series of operations into cipher text. DES uses56-bit key with 8 parity bits key for transformation, operates on 64 bits block size and includes 16 rounds.

- **Blowfish:**

Blowfish designed in 1993 by Bruce Schneier which was included in a large number of encryption products[4].Blowfish has a variable key length from 0 up to 448 bits preferably 32 to 448bits. It has a 64-bit block size and is a 16-round Feistel cipher which uses large key-dependent S-boxes. Blowfish uses round keys and all the S-boxes are generated by multiple iterations of the block cipher. This enhances the security of the block cipher, since it makes exhaustive key search very difficult, and it could be considered as the most secure symmetric algorithm [8].

- **3-Way:**

3-Way a block cipher developed in 1994 by Joan Daemen. It was considered to be very efficient in a wide range of hardware platforms. Its key length is 96 bits and it uses three 32-bit words in the algorithm for its computation, so its name is 3-Way. The block size of 3-WAY is 96 bits and is11-round S-P network[7].

- **GOST:**

GOST block cipher was established by the government of the Soviet Union as its national standardization strategy [9]. GOST has key size of 256 bits and operates over a 64-bit block size. GOST is a Feistel network of 32 rounds and is S-box based algorithm.

- **International Data Encryption Algorithm (IDEA):**

IDEA was develop by Xuejia Kai and James Massey of ETH Zurichin 1991. Originally it was called improved proposed encryption standard (IPES). The algorithm was developed as replacement of DES. It uses 52 sub keys and each of them is 16 bit long. IDEA has 64-bit block size and has 8 rounds.

- **LOKI 97:**

LOKI97 develop by Lawrie Brown, assisted by Jennifer Seberry and Josef Pieprzyk. Initially LOKI 89 and LOKI 91 were designed as replacement for DES, both of them uses 64-bit block, 64-bit key and 16 rounds of feistel cipher but they have difference in choice of particular S-box, P-box and Expansion table[10], LOKI 97 has block size of 128 bit and has variable key length i.e. 128, 192 and 256.

- **RC2:**

RC2 a symmetric key block ciphers develop by Ron Rivest in 1987, it was sponsored by Lotus for their Lotus Notes software [11]. RC2 is a 64-bit block size, variable key length and has 16 rounds.

- **RC5:**

RC5 a symmetric block cipher designed by Ronald Rivest in 1994. Author[12] describes RC5 is considered as fast block cipher and suitable for hardware implementations. RC5 has a variable number of rounds, word size and a secret key. It has heavy use of data-dependent rotations due to which differential and linear cryptanalysis attacks are not possible[13]. It suggests to use 128bit key and has variable block length 32, 64 and 128bit.

- **RC6:**

RC6 derived from RC5 and developed by Ron Rivest, Matt Robshaw, Ray Sidney, and Yiqun Lisa Yin. It is considered as an upgraded version of RC5 and provides better security against attacks as compared to RC5. It uses four registers each comprises of 32 bit and is more secure than the RC5. It has variable key length 128, 192 and 256 and is a 128bit block cipher.

- **SKIPJACK:**

Skipjack a block cipher algorithm develops by NSA. Originally it was made for use of clipper cipher[14]. Skipjack an encryption algorithm for transmission of voice data, uses deffiehelmen key exchange protocol for distribution of keys. AT&T researcher Matt Blaze, establishes a severe weakness in the Escrowed Encryption System (EES)[15], that allow a malicious party to bypass the clipper chip's escrow capability. SKIPJACK is a 64bit block cipher with a key size of 80 bits and operates over 32 rounds.

- **Tiny Encryption Algorithm (TEA):**

TEA a small code block cipher algorithm as name suggest tiny. It was designed by David Wheeler and Roger Needham of Cambridge Computer Laboratory which was presented at fast software workshop in 1994 [16] It can be included in any type of small software package, e.g. software on our phone or software for GPS in our cars [17]. It is a feistel cipher which uses operations of XOR, ADD and shift in this case. It works on confusion and diffusion properties of shannon's without need of P-Box and S-Box. TEA has 64 bit block size with a key length of 128 bit and has Feistel network structure.

- **XXTEA:**

XXTEA block cipher is a corrected version of TEA, its purpose was to overcome the weakness of TEA algorithm. XXTEA was developed by Roger Needham and David Wheeler of the Cambridge Computer Laboratory, the algorithm was presented in an unpublished technical report in October 1998[18]. It is a 64bir block cipher with a key size of 128 bit and has 32 rounds.

- **DES-X:**

DES-X a symmetric key block cipher a flavor of DES enhances the complexity of brute force by a key whitening technique. Originally DES originates in 70's having 56-bit key size and with 256 possible combination of key. A scheme was proposed to enhance the DES algorithm that was DES-X in 1984 by RivonShivest later this was included in RSA Security's BSAFE cryptography library in 19080's [19]. DES-X enhances DES by XORing its 64 bits first key (K1) to the plain text before applying any DES round and in the end XORing again with second (K2) after encryption.

- **3-DES:**

Triple DES or Triple data encryption algorithm TDEA was design in 1990's. The purpose of this algorithm was to overcome the flaws or weakness of DES. In 1998 electronic frontier foundation (EFF) broken the DES encryption in less than three days, there was a need to pick an algorithm with a longer key. There isn't enough time before sun burns out to brute-force triple DES said by famous cryptographer expert Bruce Schneier. 3DES was considered as improved version of DES in key length and repeat the procedure three times in each data block[20]. It operates over 64bit block size, 168 bit key and has 48 rounds.

- **SQUARE:**

SQUARE an iterated block cipher with a key length of 128 bits and block size of 128 bits designed by john Daeman and Vincent Rijmen. Square concentrates on the conflict against differential and linear cryptanalysis. Its design approach allow us to use higher block lengths. Design of SQUARE was published in 1997 which led to Rijndael key scheduler and was further implemented for AES [21].Basic operations of cipher are invertible transformation which are comprises of 4 x 4 array of bytes[22].

- **Twofish:**

Twofish a 128 bit block cipher with variable key length designed by Bruce Schneier, John Kelsey, Doug Whiting, David Wagner, Chris Hall, and Niels Ferguson. Twofish was considered from the top five finalist of advance encryption standard. It uses the concept of key-dependent S-Box and Pseudo-Hadamard Transform which make it strong against different attack. It has complex key schedule phenomenon and each S-Box is dependent on key[23].

- **Threefish:**

Threefish a symteric block cipher develop by bruceschneier, Niels Ferguson, Stefan Lucks, Doug Whiting, Mihirbellare, jesse walker in 2008. Threefish is same like blowfish and twofish. But, threefish uses three type of keys 256, 512 and 1024 bits and its block size is same as key size. It has 72 rounds generally but for 1024 bits it operates encryption on 80 rounds. Apart from both of them, threefish is tweakable block cipher i.e. it take three parameters as input a key, a tweak value and a block of message. The tweak value is used to encrypt block of message. Threefish doesn't use any S-Box or other table lookups in order to avoid time attack[24].

- **CAST-128:**

CAST-128 alternatively called CAST-5 is a symmetric key block cipher designed in 1996 by Carlisle Adams and Stafford Tavares. CAST-128 is a 12 or 16 rounds of feistel network and 64bit block cipher with variable key size of 40 to 128. 16 rounds of feistel networks are only implemented if 128 bit key size is used. It includes large components of 8x32-bit S-boxes which are based on key-dependent rotations, bent functions, XOR operations, and modular addition & subtraction operations [25].

- **CAST-256:**

CAST-256 also called CAST-6 is a symmetric block cipher which was published in 1998 by Carlisle Adams and Stafford Tavares. It is extension of its precedent CAST-128[26]. CAST-256 uses same procedure and operations as CAST-128 apart from few, it contains double block size as of CAST-128 and contains variable key size i.e. 128, 160, 192, 224 or 256 bit. CAST-256 works on 48feistel network rounds also called 12 quad-rounds[27].

- **Camelia:**

Camellia a 128 bit block cipher with a variable key length developed by Mitsubishi Electric. It was approved by International organization for standard (ISO) for Japanese CRYPTREC project and European Union's NESSIE project. Camellia was considered suitable for software and hardware implementations from low-cost smart cards to high speed traffic network systems[28].

- **MISTY1:**

MISTY1 or MISTY-1 a 64 bit block cipher designed by Mitsuru Matsui, Tetsuya Ichikawa, Toru Sorimachi, Toshio Tokita, Atsuhiro Yamagishi in 1995. It works with 128 bit key with variable number of rounds[29].MISTY was specialized for Mitsubishi Electric and is one of the selected algorithms used by Japanese government in CRYPTREC and European NISSIE project. But, it was dropped as candidate by CRYPREC in 2013. In 2015 after almost 20 years of failure of cryptanalytic attempts, MISTY was broken by Yosuke Todo by implementing integral cryptanalysis[30].

- **KASUMI:**

KASUMI a name originally derived from MISTY1 algorithm, a 64 bit block cipher algorithm and has 128-bit key which is optimized for hardware proficiency. KASUMI is eight round feistel network structure, round functions in feistel-like network transformation are irreversible, and each round function uses a round key consisting 16-sub keys originally derived from 128-bit key from fix key schedule [31]. KASUMI a block cipher which has been specifically used in Universal mobile telecommunication systems (UMTS), GSM and Global packet radio service (GPRS) mobile communication systems.

- **Crypton:**

CRYPTON a symmetric block encryption algorithm developed by ChaeHoon Lim is a 128-bit block cipher and it was proposed as a candidate for AES[32].CRYPTON a block cipher with variable key size of 128, 192 and 256-bit key which proves its hardware implementations are more efficient as compared to software implementation. This algorithm doesn’t uses very large operations or addition and multiplication, is simply performs XOR operations and they can be performed in parallel mode. It is SPN (Substitution-permutation network) 128-bit block cipher based on SQUARE. Each block is represented in 4x4 byte array and performs each round transformation in sequence. Whereas, each round consists of four parallel steps including column wise bit permutation, column-to-row transportation, byte-wise permutation and key addition at last. This encryption process involves 12 repetition rounds of same round transformation and decryption occurs in same manner but with different key schedule[33].

- **Information Concealment Engine (ICE):**

Information Concealment Engine (ICE) a symmetric block cipher develop by Kwan presented at Fast Software Encryption Workshop in January 1997. It is 64-bit Feistel structure similar to DES, but it introduce the concept of key-dependent permutation which led to resistance against linear and differential attacks. ICE standard version operates on 64-bit block and takes 64-bit key with 16 sub-keys in 16 rounds. A fast version namely Thin-ICE operates over 64-bit block with 8 rounds and 64-bit key and open ended variants ICE-n uses 16n rounds and 64n-bit keys. ICE take 64-bit plaintext as input and spilt it into two halves i.e. 32-bit. Every round of function F take right half of 32-bit and a 60-bit sub-key and the output of this is XORed with left half and then they are swapped with each other. The Expansion function, keyed permutation, Xor operations, S-boxes, permutation function and key schedule repeats for all round but in final round where the swap is left out, the two halves are concatenated and cipher text is formulated[34].

3. Related Work:

This section discusses the results and information that is obtained from different sources and previous work done in the field of cryptographic algorithms. Previously different work has been done by comparing algorithms on various parameters like encryption and decryption speed, power consumption, memory utilization.

Author of [24] has done comparison on symmetric key encryption algorithms. A fair comparison among five algorithms like Blowfish, RC2, RC5, Two Fish, and Three Fish is done. Authors concluded that among these five algorithms Three Fish algorithm uses variable number of bits ranges from 256-1024 and it encrypts data 72 times, which makes the data impossible to be decrypt or hacked.

In paper[35]authors have compared the performance of Blowfish and Skipjack. Both of these were implemented using Microsoft Visual and .Net Framework, varying different file size and its content. Authors concluded result which shows that Blowfish is faster than Skipjack. However, security wasn’t considered as a metric during their experiment. They only consider performance in terms of encryption and decryption time.

In paper[36] authors have done comparison among different techniques of cryptography. Authors analyzed the performance of symmetric and asymmetric algorithms on basis of multiple parameters like encryption and decryption time, key generation time among different file sizes. The experiments were conducted on Java Platform by concluding that symmetric techniques are computationally inexpensive then asymmetric techniques.

In paper[37]authors have compared the performance of secret key encryption algorithms i.e. DES, 3DES, Blowfish and AES. Authors have compared the performance in terms of measuring execution times by using different block cipher modes on two different hardware platforms. At the end, results were analyzed and authors concluded that Blowfish is fastest algorithm among all of them.

In paper[38]authors have done comprehensive comparative analysis of different symmetric cryptographic algorithms based on different parameters. Authors concluded the objective of their work, to analyse the performance in terms of scalability, flexibility, reliability, robustness and security. Authors highlight the limitations of symmetric and asymmetric algorithms which are considered as essential parameters for secure wireless or wired communication. During the analysis, they also figured out that Rijndael algorithm was considered most suitable in terms of security, flexibility, and memory usage and encryption performance as compared with others algorithms which are being compromised by few of these characteristics.

In paper[37] authors have compare the performance of two encryption algorithms i.e. AES and DES. They analyze the performance in terms of processing time, CPU utilization, and encryption throughput on two different operating systems i.e. MAC and Windows. The simulation was performed on visual basic .NET 2013 version, which concluded that AES is faster than DES in execution time for the two platforms and has high throughput, whereas DES has less CPU utilization on both of the platform.

In paper[4]authors have done comprehensive evaluation of cryptographic algorithms namely DES, 3Des, Blowisfish, RSA and AES. They evaluated the performance of algorithms by measuring multiple parameters i.e. encryption and decryption time, memory used, avalanche effect and entropy (randomness). Authors concluded that each algorithm has its limitations and strength, in order to apply cryptographic algorithm to any application we should have sound knowledge regarding its performance, strength and its weakness. From experimental analysis, Blowfish consumes less memory for implementation in any of application as compared to other algorithms and Blowfish is suitable to be implemented in software platforms where time and memory is major aspect. For cryptographic strength AES is best and where network bandwidth is required DES is considered to be best suited algorithm.

In paper[39] authors have analyze the performance and efficiency of different cryptographic algorithms namely DES, 3DES, CAST-128, RC2, Blowfish and IDEA. They have compared the performance by analyzing multiple parameters in different input data formats. I.e. text, audio and video. After analyzing results authors concluded that 3DES has more power consumption, CAST-128 has better throughput and RC2 can be implemented for smaller data whereas, Blowfish has least power consumption as compared to others and hence they concluded that Blowfish has better performance and efficiency in all perspective.

4. Comparative Study:

Table1: Comparison of modes with Multiprocessing factors among various algorithms

Algorithms	Modes	Parallel multiprocessing	Key size increase/decrease
DES	Yes CBC,CFB,ECB OFB	No	Initial 64 to 56 bit
3-DES	Yes	No	Three times increase then DES
AES	Yes, CTR	No	Variable
BlowFish	EBC,CBC	No	Variable
GOST	OFB, CFB	No	No
B-REA	CBC	Yes	No
SERPENT	N/A	Yes	Variable
Square	N/A	yes	Variable
Shark	N/A	Yes	Fixed
IDEA	N/A	Yes	Fixed
CRYPTON	N/A	Yes	Variable

Table 2: Comparison of Recursive and S-Box Dependent data Operations

Algorithms	Recursive nature	Galois field (finite field)	Key dependent S-Box
DES	No	No	No
3-DES	Yes	No	No
AES	Yes, In transformation rounds. Varies with key	Yes, (Round constant)	No
Blowfish	No	No	Yes
Two-fish	No	No	Yes
Three-fish	No	No	No
RC5	No	No	No
MRVLK	N/A	N/A	Yes
Khufu	No	N/A	Yes

Table 3: Comparison among randomness nature and expansion table

Algorithms	Random key	Key table expansion	S-box
B-REA	Yes	No	No, Mono-alphabetic substation
RC5	No	Yes	No
IDEA	No	No	No
CAST	No	No	Yes [51]
Blowfish	No	Yes up to 448 into sub-keys	No, data dependent substitution
Three-fish	No	Nos	No S-Box
MRVLK	Yes	N/A	Yes
PRESENT	No	N/A	yes

Table 4: Comparison of Cryptographic primitives and their security

Algorithm	Cryptographic Primitives	Encryption Primitives	Source	Security services
DES	Confussion,Diffussion	Substitution, Permutation	IBM, enhanced by NSA	Confidentiality
AES	Confussion,Diffussion	Substitution, Shift, Bit Mixing	Independent Dutch cryptographers	Confidentiality
CAST	N/A	Substitution, Bit rotation	Developers, supported by Canadian Government	Confidentiality
TEA	Confusion, Diffusion	XOR, ADD, Sift	Independent cryptographers	Confidentiality
Blowfish	Confusion, Diffusion	Substitution	Independent cryptographers	Confidentiality

Table 5: Comparison among Dynamic nature of algorithms

Algorithm	Dynamic Key Schedule	Dynamic S-Box
MRVL	☑	×
DES	×	×
AES	×	×
RC5	×	×
Random PRESENT	☑	☑
VBEDM	☑	×

Table 6: Comparison of data dependent values

Algorithm	Iterated Bock Ciphers	Tweak Value	Key-Data Dependent Rotations
ThreeFish	×	☑	×
Square	☑	×	☑
Curupira-1	☑	×	×
IDEA	×	×	×
RC5	×	×	☑

Table 7: Comparison of keyed values and constraint resources

Algorithm	Cyclic Key Schedule	Key Dependent Permutation	Constrained Resources
FEAL	×	×	☑
Curupira	×	×	☑
ICE	×	☑	☑
CRYPTON	×	×	☑
KASUMI	×	×	☑
AES	☑	×	×
MISTY	×	×	☑

5. Conclusion and Future Directions:

Information security is becoming a main cause of attention now-a-days and cryptography plays very important role in it. By applying cryptographic algorithms, security can be enhanced in every field. In this research different symmetric cryptographic algorithms have been discussed and a comparative study among multiple parameters has been performed. Each algorithm has its own strengths and weakness and its benefit comparable among multiple parameters. Multiple parameters of different nature are discussed i.e. static, variable and dynamic. Before applying cryptographic solution to any domain or environment, there’s a need to have knowledge about the nature of algorithms. Hence, this study is carried out on this basis and will be beneficial in all aspects.

References

[1] M. Agrawal and P. Mishra, “A comparative survey on symmetric key encryption techniques,” Intern. J. Comput. Sci. Eng., vol. 4, no. 5, pp. 877–882, 2012.

[2] G. Singh et al., “Cryptography : A Comparative Analysis for Modern Techniques,” Int. J. …, vol. 1, no. 2, pp. 1997–1999, 2017.

[3] Z. Hercigonja, D. Gimnazija, and C. Varazdin, “Comparative Analysis of Cryptographic Algorithms and Advanced Cryptographic Algorithms,” Int. J. Digit. Technol. Econ., vol. 1, no. 2, pp. 1–8, 2016.

[4] P. Patil, P. Narayankar, D. G. Narayan, and S. M. Meena, “A Comprehensive Evaluation of Cryptographic Algorithms: DES, 3DES, AES, RSA and Blowfish,” Procedia Comput. Sci., vol. 78, no. December 2015, pp. 617–624, 2016.

[5] P. Kumar and S. B. Rana, “Development of modified AES algorithm for data security,” Optik (Stuttg)., vol. 127, no. 4, pp. 2341–2345, 2016.

[6] “Data Encryption Standard,” Wikipedia. [Online]. Available: https://en.wikipedia.org/wiki/Data_Encryption_Standard.

[7] S. Singh and R. Maini, “Comparison of data encryption algorithms,” Int. J. Comput. Sci. …, vol. 2, no. 1, pp. 125–127, 2011.

[8] D. Zhu and D. Zhu, Profiling Symmetric Encryption Algorithms for Profiling Symmetric Encryption Algorithms for by. Faculty of Electrical Engineering, Mathematics and Computer Science Delft University of Technology II.

[9] Wikipedia, “GOST (block Cipher).” [Online]. Available: https://en.wikipedia.org/wiki/GOST_(block_cipher)#cite_note-std2015-1.

[10] “LOKI,” Wikipedia. [Online]. Available: https://en.wikipedia.org/wiki/LOKI.

[11] “RC2,” Wikipedia. [Online]. Available: https://en.wikipedia.org/wiki/RC2.

[12] R. L. Rivest, “The RC5 Encryption Algorithm * A Parameterized Family of Encryption Algorithms.”

[13] S. Charbathia and S. Sharma, “A Comparative Study of Rivest Cipher Algorithms,” Int. J. Inf. Comput. Technol., vol. 4, no. 17, pp. 1831–1838, 2014.

[14] “Skipjack_(cipher),” Wikipedia. [Online]. Available: https://en.wikipedia.org/wiki/Skipjack_(cipher).

[15] “SKIPJACK-NSA Type 2 cryptographic algorithm,” Crypto Museum. [Online]. Available: http://www.cryptomuseum.com/crypto/usa/skipjack.htm.

[16] “Tiny Encryption Algorithm,” Wikipedia. [Online]. Available: https://en.wikipedia.org/wiki/Tiny_Encryption_Algorithm.

[17] D. J. Wheeler, R. M. Needham, E. D. Wheeler, and R. Needham, “TEA , a Tiny Encryption Algorithm,” Elsevier.

[18] “XXTEA,” Wikipedia. [Online]. Available: https://en.wikipedia.org/wiki/XXTEA.

[19] “DES-X,” Wikipedia. [Online]. Available: https://en.wikipedia.org/wiki/DES-X.

[20] M. F. Mushtaq, S. Jamel, A. H. Disina, Z. A. Pindar, and N. S. Ahmad, “A Survey on the Cryptographic Encryption Algorithms,” nternational J. Adv. Comput. Sci. Appl., vol. 8, no. 11, pp. 333–344, 2017.

[21] “Square (cipher),” Wikipedia. [Online]. Available: https://en.wikipedia.org/wiki/Square_(cipher).

[22] J. Daemen, L. Knudsen, and V. Rijmen, “The Block Cipher SQUARE,” in Fast Software Encryption. FSE, 2006, pp. 149–165.

[23] S. S. Ali and D. Mukhopadhyay, “Differential Fault Analysis of Twofish,” in International Conference on Information Security and Cryptology, 2013, pp. 10–28.

[24] G. Muthukumar, “A Comparative Analysis on Symmetric Key Encryption Algorithms,” Int. J. Adv. Res. Comput. Eng. Technol., vol. 3, no. 2, pp. 379–383, 2014.

[25] Y. Mahamat, S. H. Othman, M. Siraj, and H. Nkiama, “Comparative Study Of AES , Blowfish , CAST-128 And DES Encryption Algorithm International organization of Scientific Research International organization of Scientific Research,” IOSR J. Eng., vol. 6, no. 6, pp. 1–7, 2016.

[26] H. M. Heyst and S. E. Tavaresj, “An Analysis of the CAST-256 Cipher,” in 1999 IEEE Canadian Conference on Electrical and Computer Engineering, 1999, pp. 361–366.

[27] S. Wang, T. Cui, and M. W. B, “Improved Differential Cryptanalysis of CAST-128 and CAST-256,” in International Conference on Information Security and Cryptology, 2017, no. June 1998, pp. 18–32.

[28] K. Aoki, T. Ichikawa, M. Kanda, and M. Matsui, “a,” in International Workshop on Selected Areas in Cryptography, 2001, pp. 39–56.

[29] M. Matsui, “New Block Encryption Algorithm MISTY,” in International Workshop on Fast Software Encryption, 1997, pp. 54–68.

[30] A. Bar-on and R. Gan, “A 270 Attack on the Full MISTY1,” pp. 1–23, 2015.

[31] K. Jia, L. Li, C. Rechberger, J. Chen, and X. Wang, “Improved Cryptanalysis of the Block Cipher KASUMI,” Springer, pp. 222–233, 2013.

[32] C. H. Lim, “CRYPTON : A New 128-bit Block Cipher { Specification and Analysis {,” Inf. Commun. Res. Center; Futur. Syst. Inc., 1998.

[33] E. Hong, J. Chung, and C. H. Lim, “Hardware Design and Performance Estimation of the 128-bit Block Cipher CRYPTON,” in International Workshop on Cryptographic Hardware and Embedded Systems, 2001, pp. 49–60.

[34] M. Kwan and M. Kwan, “The Design of the ICE Encryption Algorithm,” in International Workshop on Fast Software Encryption, 2006.

[35] A. Ahmad Milad, H. Zaiton Muda, Z. A. Bin Muhamad Noh, and M. Almahdi Algaet, “Comparative Study of Performance in Cryptography Algorithms (Blowfish and Skipjack),” J. Comput. Sci., vol. 8, no. 7, p. 91, 2012.

[36] M. M. Ali, “Cryptography : A Comparative Analysis for Modern Techniques,” vol. 8, no. 6, pp. 442–448, 2017.

[37] S. D. Rihan, S. E. F. Osman, and A. Khalid, “A Performance Comparison of Encryption Algorithms AES and DES,” Intetnational J. Eng. Res. Technol., vol. 4, no. 12, pp. 151–154, 2015.

[38] M. Ebrahim, S. Khan, and U. Bin Khalid, “Symmetric Algorithm Survey: A Comparative Analysis,” vol. 61, no. 20, pp. 12–19, 2014.

[39] I. Alam and M. R. Khan, “Performance and Efficiency Analysis of Different Block Cipher Algorithms of Symmetric Key Cryptography,” Int. J. Adv. Res. Comput. Sci. Softw. Eng., vol. 3, no. 10, pp. 713–720, 2013.

Table 8: Comparison of general description of various algorithms

Algorithm	**Key**	**Block**	**Rounds**	**Rotations**
DES	64 bit initial then 56 bit	64 bit fixed block/ S-Box Fixed	16	Fixed
3DES	3x56	Same size.	48	Fixed
RC1	Not implemented	Not implemented	N/A	N/A
Rc2	Variable sized key	64 bit block	18 rounds, fiestel network	Fixed
Rc3	Not secured	Not secured	N/A	N/A
Rc5	0 - 2040 bits key size, suggested is 64 bit	Variable 32, 64, 128, suggested is 128 bit-key	0-255, suggested is 12 rounds.	Data dependent
Rc6	128, 192, 256, key must be multiple of 32 bits	0 to 2040 bits (128 suggested)	20	Data dependent rotations
Blowfish	32 to 448 recommended is 128, must be multiple of 32	64 bit	16 rounds, each round depends on key dependent permutation	N/A
Twofish	Upto 256 bits	128 bit	16	N/A
Three-fish	256, 512, 1024 bits	Key size equal to block size	72 rounds	N/A
IDEA	128 bit	64 bit	8.5	N/A
CAST	40-128, used when key is 80 bits	64 block	12-16 , full 16 used when key is greater then 80 bits	Key dependent
PRESENT	80 bit and 128-bit key	64-bit block	31 rounds	N/A
SERPENT	128,192, 256	128 bit	32 bit round base on four bloack of 32 bits	N/A
AES	128, 192, 256	128	Key dependent rounds	Fixed
MRVLK	Random Variable key selection depends on message	Variable block length	Variable	Random bitwise rotation (data dependent)
VBEDM[59]	Not fixed, Unlimited key size	Variable block for each round	Variable	N/A
Crypton	Variable key size 128, 192 and 256 bit	128-bit	12	Fixed
ICE	64 bits	64 bits	8	Fixed
SQUARE	128 bits	128 bits	8	Iterated block cipher