Tuijin Jishu/Journal of Propulsion Technology
ISSN: 1001-4055
Vol. 44 No. 3 (2023)

Comparative Analysis of Multi-Level Algorithm with Different Encryption and Decryption Security Algorithms

Dr. Gaurav Aggarwal
Professor & Dean, Dept. of CSE, Jagannath University, Bahadurgarh (Jhajjar), Haryana, India
ORCID iD: 0000-0002-6836-9352, Email Id:- gauravaggarw@gmail.com

Mr. Hirdesh Sharma
Research Scholar**,** Jagannath University, Bahadurgarh (Jhajjar), Haryana, India
ORCID ID**:** 0000-0002-1278-4135**,** Email Id:- hirdesharma@gmail.com

Abstract

This research explores network data encryption and decryption strategies used in communication networks. The majority of network communication systems revolve around information sharing on mobile phones, networked PCs, and other internet-connected electronic devices. As information travels through several networks and is subject to numerous types of assaults, unsecure data can be read, altered, or faked by anybody with access to it. To defend against this form of assault, data encryption / decryption techniques are utilized. To illustrate the effects and evaluate the efficacy of each decoding and encryption method used in network technologies, Visual Basic simulation studies that encrypted and decrypt data were created, developed, and tested. Further study was for comparative analysis of Multi-Level Algorithm with different Security Algorithms for encrypting data approach.

keywords: DES, AES, RSA, DSA, Cipher text, Symmetric encryption, Asymmetric encryption.

1. INTRODUCTION

By transforming data or information into an unintelligible code, encryption, a special form of cryptography, enables data or information to be hidden. In encryption, the data transformation is frequently done using a preset parameter or key. While certain encryption algorithms require that the message and the key have the exact same length, other encryption schemes can work with keys that are far shorter than the message. The most common places where encryption is used are on insecure communication channels, like automated teller machines (ATMs), mobile phones, the internet and many more. By using encryption to create digital signatures, messages can be authenticated. Data is converted back to its original form via decryption, which functions as encryption's opposite.

A. Symmetric Encryption

Symmetric encryption, which simultaneously encrypts and decrypts data, uses a single key. Thus, the key must be sent to the recipient in order for them to be able to decode the communication. Traditional cryptosystems including AES, Blowfish and DES are often used by the Federal Government.

When the keys for encryption and decryption match.

$$P=D\ (K,\ (E\ (K,\ P)).$$

Advanced Encryption Standard (AES): Instead than utilising DES, NIST advises switching to the more recent encryption technology AES. The top encryption standard was selected in 1997, and it is called the Rijndael algorithm (pronounced "rain doll"). Federal Information Processing Standard Number 197 from 2001 specifies the symmetric cypher as the encryption technique that the federal government has approved. Both 128-bit and 192-bit AES can be used up to SECRET level and TOP SECRET level, according to the National Security Agency. AES was built on the Rijndael algorithm, which was developed by Joan Daemen and Vincent Rijmen. 128 bits, 192 bits, and 256 bits are the three allowed key lengths offered by AES. It is only known to be resistant to brute force attacks, when an attacker attempts each character.

(i) **Blowfish:** It is one of the most well-liked publicly available encryption algorithms provided by a prominent cryptologist and president of Amount of surface Systems, a company that specialises in information security and cryptography consultancy. This strategy, which is mostly used in application software and has the drawback of weak keys, can be improved for use in hardware devices and has not yet been successfully attacked. A block cypher with 64 bits and variable-length keys is called blowfish.

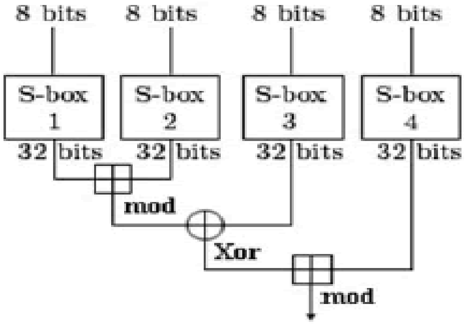


Figure1. Blowfish Function

(ii) **Data Encryption Standard (DES):** The encryption method advised by NISTfirst was DES. It is inspired on the Lucifer algorithm suggested by IBM. The use of DES as a regular encryption method for sensitive but declassified data was authorised by the federal government in 1977. And since, DES has become the subject of a variety of assaults and strategies that take advantage of its vulnerabilities, making it a dangerous block cypher. DES, which is widely used, was thought so difficult to decrypt that export to other countries was forbidden by the United States government. DES employs a private (secret) key to protect the data.

B. Asymmetric Encryption

Asymmetric encryption, often known as public-key encryption, uses two different keys—the public key—to encrypt and decrypt information. This allows users to freely distribute the public key to everyone they predict would wish to communicate with them as only those who have the private key can decode a message. Information is encrypted and decrypted between two users when it is sent or received. The sender uses the user's public key to encrypt the data and the user's private key to decrypt it. EL-GAMAL, Digital Signature (DSA), and Rivest, Adi Shamir, and Leonard Adleman (RSA) are three good examples of asymmetric encryption methods.

When the keys are different.

$$P=D\ (Kd,\ (E\ (Ke,\ P)).$$

(i) **Digital Signature (DSA):** Digital signatures are used to verify the source and content of messages, and they are implemented using public-key encryption. Since that even the slightest change to the message results in several appearances in the message digest, the receiver of a digital signature is able to verify that the message genuinely came from the sender.

(ii) **Rivest, Adi Shamir, and Leonard Adleman (RSA):** The RSA encryption and authentication method used on the Internet is built on an algorithm developed in 1977 by Ron Rivest, Adi Shamir, and Leonard Adleman. The most used authentication and encryption method is the RSA algorithm, that's a part of the Microsoft & Netscape Web browsers. It is present in numerous programmes, including Quicken & Lotus Notes from Intuit. RSA Security is the proprietor of the encryption scheme. The company sells development kits in addition to granting licences for algorithm technology. The technologies are indeed a part of computing, Web, and Internet standards that are actively being created or suggested.

2. RELATED WORK

The associated research includes, but is not limited to:

(a) In order to improve data protection, Navneet and Vijay (2012) produced a study titled "Different Data Encryption Techniques Used in Secured Auto Teller Machine Transactions" that covered a variety of encryption methods and guidelines. Data security is a top priority in today's banking and financial activities, especially when sensitive and protected data is being shared.

(b) The most recent authentication, according to Kanaljit's (2011) study, Safeguarding Computer Network with Encryption Method, includes biometric applications like fingerprints and retina scans. The protection of sensitive data is one of the most important issues facing organisations today, as well as their customers. Due to this and growing regulatory obligations, organizations are under demand to preserve the security, confidentiality, and integrity of critical information.

(c) Authentication and encryption, as according research on encryption methods of data safety for wireless sensor networks conducted by Qingzhang and Zhongzhe, are the two most important modules in the wireless sensor network's data protection (2011). Yet, while implementing security measures, sensor nodes with constrained processing and storage capabilities must consider their storage space, power needs, and other factors.

(d) Vinod and Niranjan's Mechanism for Message Encryption and Decryption (2011). Their study presents a simple and reliable encryption method that makes use of substitution mapping, translating, and transposition procedures.

3. BACKGROUND OF ENCRYPTION AND DECRYPTION ALGORITHMS

CRYPTOGRAPHY is an analytical process that turns a plain text or plaintext communication into the cipher text or cypher information using an encryption method.

(a) **Types of cryptographic algorithms**- Several different methods can be used to arrange cryptographic algorithms. The three types of algorithms that are discussed are as follows.

- Secret Key Cryptography (SKC): Using this technique, data is encrypted and decrypted with the same key.
- In public key cryptography, one key serves as the encryption key and a second for decryption (PKC).
- Hash Functions: a mathematical procedure is used to irreversibly "encrypt" data.

(b) **Symmetric Key Cryptography: -** The most widely used symmetric key encryption method is the DES, which was published around 1977 by the National Bureau of Standards. DES The most common symmetric-key approach is still this one. With the use of a strong algorithm and a fixed length, 56-bit key, it quickly encrypts and decrypts communications. The hardware implementation is straightforward, hastening the process of decryption and encryption. In general, increasing the key size makes the system safer. A DES version called Triple-DES, commonly referred to as DES-EDE (encrypt-decrypt-encrypt), uses three DES applications and two different DES keys to produce an effective key size of 168 bits [ANSI 85].

(c) **Asymmetric key cryptography,** or By using numerous decryption and encryption key pairs, public/private key cryptography addresses the key management problem. Having one key—say let us its encryption key—does not allow one to ascertain the second key, the decryption key. The encryption key therefore can be publicly disclosed (hence the name “public/private key cryptography”) because only the party wishing to obtain encrypted messages is in knowledge of the decryption key. With the public key, anybody can encrypt a communication, but only the intended receiver can decrypt it.

4. **A Hash functions**, a sort of one-way function, are used extensively in cryptography. While one-way functions are easy to calculate, they can be tricky to invert. Given the function’s result, it is difficult to discern its input. It is feasible to define “easy” and “hard” mathematically. With a few notable exemptions, almost the entire field of cryptography using public keys relies on the availability of one-way functions.

4. STUDIES AND FINDINGS

Symmetric or secret key cryptography Stream cyphers and block cyphers are both of the main categories of secret code encryption methods. In stream cyphers, the key is constantly changing thanks to a feedback mechanism. They focus on one bit at a time (or byte, or computer word).

(d) Encryption algorithm

Step 1: Create the ASCII value of the letter;

Step 2: Create the binary value of the letter. [Binary values must have 8 digits; the decimal 32 number in binary must be 00100000.]

Step 3: The eighth binary number is inverted.

Step 4: Enter a 4-digit divisor (more than 1000) as your key.

Step 5: Subtracting the factor from the reversible number

Step 6: Maintain the remainder of the number in the first three digits and the percentage in the next five (the remainder and quotient cannot be longer than three and five digits, respectively). If any of these are less than 3 or 5 digits, we must add a sufficient amount of 0s to the left side.

(b) Decryption algorithm

Step 1: The encrypted text’s last 5 digits must be divided by the Key.

Step 2: Add the first three digits of the cypher text to the response you got in step one.

Step 3: We must convert the output of step 2 into an 8-bit number if the outcome is not an 8-bit number.

To get the original content, or plain text, inverse the number you entered in step 4 instead.

(c) Public key cryptography

One of the earliest public-key cryptosystems to be used in actual everyday situations for safe transmission of data is the well-known RSA. This kind of cryptosystem uses an encryption key that is public rather than a private decryption key. Due to the practical difficulties of addressing the factoring problem—which is the product between two enormous prime integers—RSA exhibits this asymmetry. The approach was created in 1977 by Leonard Adleman, Ron Rivets, and Adi Shamir, who are collectively referred to as RSA. English mathematician Clifford Cocks developed an equivalent technique in 1973, but it wasn't declassified until 1997.

A user of RSA creates a public key, publishes it, and then bases it on two large prime integers and an auxiliary value. We must maintain the secrecy of the prime numbers. Anyone can encrypt a message with the public key, but 1644tilized1644 the techniques which have been made visible so far, when the public key is large enough, only a single individual who is knowledgeable of the most important variables will be able to read the message. Decoding an RSA key is what causes the RSA problem. It is a great question as to whether it is just as difficult as the factoring problem.

(e) Key generation

RSA uses both public and private keys. The public key is made available to the public and can be 1644tilized to encrypt messages. The private key alone can reliably and rapidly decrypt communications that have been encrypted using the public key. The RSA method's keys are created using the process described below.

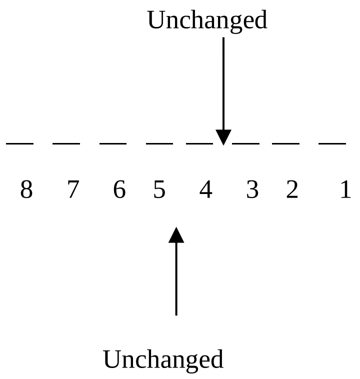
(f) I Cryptographic Hash function

Hash functions, a category of one-way functions, are significantly used in most cryptography. In this application, a function's description and evaluation are based on how resilient it is to an adversary assault. If it is computationally difficult to locate a message y that is not equivalent to x such that H(x) = H(y), then the message x is considered to be a weak collision-free hash function. One needs a robustly collision-free hash function H. (y) in order to find any pair of messages x and y such that H(x) = H. The specifications for an efficient cryptographic hashing algorithm are more strict than for many other applications (error corrections and audio recognition are excluded). Because of this, stock hash algorithms like MD5 and SHA-1, which have had their cryptographic security compromised, are nevertheless effective. But the SHA-2 algorithm has no known vulnerabilities. A function with additional security properties, such as message integrity and authentication, can be referred to as a "hash function" and used as a primitive in a range of information security applications. It may take in lengthy strings (or message) of any length and produces strings with a predetermined length that are sometimes referred to as digests of messages or digital fingerprints.

5. Performance Analysis of Different Encryption Algorithms

Time Complexity of Developed Algorithm: As we discussed earlier our algorithm has following encryption steps.

- Bit
- Character
- Word
- Line
- Paragraph



Have total no of bits 8 and no of swap 3. So time complexity for one character will be O(3). In general time complexity for one character will be O(S).

Where S=3

Now a word has 8 characters. So time complexity for one word will be O(3*8) and a line has 8 words. So time complexity for one line will be O(3*8*8). A paragraph has 8 lines. So time complexity for one paragraph will be O(3*8*8*8) i.e. O(3*8^3).

Now define a general term. A message has N paragraph, which has to be encrypted. So total message can be divided into paragraph, line, word as well as characters. So message can be represented as

Message size = N paragraph
=N*8 Lines OR
=N*8*8 Words OR
=N*8*8*8 Characters OR
=N*8*8*8*8 Bits

So total running time to encrypt message M will be O (3*8*8*8*8*N) i.e. O (3*8^4*N).

TC← C*N

Where C=3*8^4.

Now this time complexity can be bounded.

TC←C*N

TC=O (N)

Complexity of Existing Algorithm: Complexity for the new multi-level algorithm will also be **O (N).** Decryption and encryption processes can thus be finished in a linear amount of time.

S.No.	Name of Encryption Algorithm	Best Case	Average Case	Worst Case
1.	**Encryption algorithm**	O(n log(n))	O(n log(n))	O(n^2)

2.	**Decryption algorithm**	O(n log(n))	O(n log(n))	O(n log(n))
3.	**Public key cryptography**	O(n log(n))	O(n log(n))	O(n log(n))
4.	**Key generation**	O(n)	O(n log(n))	O(n log(n))
5.	**Cryptographic hash function**	O(n)	O(n^2)	O(n^2)
6.	**Multi-level algorithm**	O(n)	O(n)	O(n)

Table 1: Performance of different algorithms

Multi-level Encryption Algorithm for Computer Networks

Computer networks employ the multi-level encryption method for security. Compared to current security methods like WEP (Wireless Equivalent Privacy), 802.1X, and others, this technique is considerably different. It is possible to attain the same security efficacy of earlier predecessor algorithms by taking Quality of Protection (QoP) into serious account. Depending on the level of protection desired, the procedure can be applied at several levels. Four levels make up this level of security, three of which depend on block cyphers and the fourth on a stream cypher method. The algorithm can be used for decompression with various and additional difficulties because it was built using a symmetric key approach. For the protection of plain text data, a multidimensional method with four dimensions has been created.

Performance Evaluation of Symmetric Encryption Algorithms

Applications for the internet and networks are expanding quickly, so there is a greater need to defend these applications. In information security systems, encryption methods are crucial. On the other hand, those algorithms need a lot of computational resources, including memory, CPU time, and battery power. Here, we compare six of the most used symmetric encryption algorithms, including RC6, DES, 3DES, AES (Rijndael), RC2, and blowfish. To illustrate each algorithm's effectiveness, simulation results are provided.

The results of the simulation allow us to draw several conclusions. First, there is no discernible difference between the findings given in base 64 encoding and hexadecimal base encoding. Second, it was determined that Blowfish performs better than other widely used encryption algorithms in the event of increasing packet size, followed by RC6. Third, it was discovered that RC2, RC6, and Blowfish had a disadvantage over the other algorithms with regard to of time consumption when switching from text to another sort of data, such as an image.

Comparative Analysis of the Hardware Implementations of Hash Functions SHA-1 and SHA-512

A number of cryptographic systems and security protocols, including IPSec and SSL, presently utilise hash functions [6], one of the most used cryptographic primitives. We compared the latest strong hash standard, SHA-512, with the previous standard, SHA-1, using hardware implementations. In our implementation using Xilinx Vertex FPGAs, SHA-512 has a throughput of 670 Mbit/s compared to SHA-1's 530 Mbit/s. Our analysis demonstrates that the recently proposed hash standard is additionally noticeably faster than the previous standard, but also orders of magnitude more secure. Both hash functions' basic iterative architectures are quicker than symmetric-key cyphers' basic iterative architectures for similar security.

The newly proposed draught hash standard SHA-512 has been implemented on an FPGA, and its performance has been compared to that of the previous hash standard SHA-1. We made an attempt to employ the same design and technology and optimisation methods throughout. According to the static timing analysis and the testing, our solutions based on the Xilinx XCV-1000-6 demon show that SHA-512 is 26% faster than the equivalent implementation of SHA-1. In addition, SHA-512 uses two more 4 kbit Block RAMs and nearly twice as many CLB slices than SHA-1 without accounting for an input/output interface. These findings have been experimentally confirmed using the PCI FPGA Board, SLAAC-1V, which is built around three Virtex 1000 FPGA chips from Xilinx. Our findings demonstrate that there is no need to compromise cryptographic security for hardware speed when designing a powerful hash function. However, the more robust hash function can necessitate a significant increase in hardware resources. Additional loop unrolling-based optimisations of both systems are doable and will be described in a subsequent publication. Our study is a component of a broader project to implement the recently published cryptographic algorithms of IPSec as a gigabit rate hardware accelerator on a PCI card based on Xilinx FPGA.

6. CONCLUSION

Communication security relies on encryption algorithms, and the three main concerns are battery life, memory utilisation, and output byte. Performance testing is done using the chosen encryption techniques AES, DES, and RSA. The chosen algorithms are RSA and DSA for asymmetric encryption and AES, DES, and Blowfish for symmetric encryption. We can reach a number of conclusions based on the simulation's results. First of all, there is no appreciable difference between the data reported in base 64 or hexadecimal base encoding. Second, it was discovered that in the case of growing packet size, Blowfish outperforms other popular encryption methods, followed by AES. Third, it was revealed that Blowfish was slower than other algorithms when moving from text to other types of data, such images. There are various data encryption methods, like symmetric encryption, that encrypts and decrypts information using just one key (the encryption key). Important information must be encrypted.

REFERENCES

1. Marshall Ball, Dana Dachman-Soled, & Mukul Kulkarni. (2020). New techniques for zero-knowledge: Leveraging inefficient provers to reduce assumptions, interaction, and trust. Daniele Micciancio and Thomas Ristenpart, editors, CRYPTO2020, PartIII, volume 12172 of LNCS, pages 674–703. Springer, Heidelberg.
2. Shohei Egashira, Yuyu Wang, & Keisuke Tanaka. (2019). Fine-grained cryptography revisited. StevenD. Galbraith and Shiho Moriai, editors, ASIACRYPT2019, PartIII, volume 11923 of LNCS, pages 637–666. Springer, Heidelberg.
3. Saarinen, M-J; Aumasson, & J-P. (2015). The BLAKE2 Cryptographic Hash and Message Authentication Code (MAC). IETF. doi:10.17487/RFC7693. RFC 7693. Retrieved 4.
4. Deepak K. D. and Pawan D.,―Performance Comparison of Symmetric Data Encryption Techniques‖ ISSN: 2278 – 1323 International Journal of Advanced Research in Computer Engineering & Technology Volume 1, Issue 4 June 2012.
5. Rivest, R. L., Shamir, A., & Adleman, L.―Methods for Obtaining Digital Signatures and Public key cryptosystems‖, communication Of the ACM Vol. 21. pp. 120—126.1978.
6. Deepak K. D. and Pawan D.,―Performance Comparison of Symmetric Data Encryption Techniques‖ ISSN: 2278 – 1323 International Journal of Advanced Research in Computer Engineering & Technology Volume 1, Issue 4 June 2012
7. S.Kumari and J. Chawla, Comparative Analysis on Different Parameters of Encryption Algorithms for Information Security, International Journal of Innovations & Advancement in Computer Science (IJIACS), Volume 4, Special Issue, pp. 123-129, 2015

8. S. Gurpreet and Supriya,A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information SecurityInternational Journal of Computer Applications, Volume6, Issue 19, pp. 33-38, 2013.
9. S.Lalit and R.Bharti, Comparison among different Cryptographic Algorithms: Neighborhood-Generated Keys InternationalJournal of Computer Applications (0975 – 8887), Volume 73, Issue 5, pp. 144-153, 2013.
10. S. Neetu, Cryptanalysis of Modern Cryptographic Algorithms: International Journal of Computer Science and Technology,Volume 1, Issue 2, pp.166-169, 2012.
11. M. Mini and S.Aman,Study of Various Cryptographic Algorithms. International Journal of Scientific Engineering and Research (IJSER) www.ijser.in ISSN (Online): 2347- 3878, 1 (3): pp.1667-1672, 2013.
12. S. Pavithra, and E.Ramadevi, (2012). Performance Evaluation of Symmetric Algorithms: Journal of Global Research in Computer Science, 3 (8): 43-45.
13. Pasmavathi B. and Ranjitha S.A Survey Performance Analysis of DES, AES and RSA Algorithm along with LSB Substitution Technique: International Journal of Science and Research (IJSR) Volume 2, Issue 4, pp. 170-174,2013.
14. "Announcing the ADVANCED ENCRYPTION STANDARD (AES)". United States National Institute of Standards and Technology (NIST). November 26, 2001. http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf. Retrieved October 2,2012.
15. Federal Information Processing Standards Publication (FIPS) 180-4, “Secure Hash Standard” March 2012, [online] available at: http://csrc.nist.gov/publications/fips/fips180-4/fips-180-4.pdf [accessed 20 August 2012].
16. Sean O’Melia and Adam J. Elbirt, 2010 “Enhancing the Performance of Symmetric-Key Cryptography via Instruction Set Extensions” IEEE Transactions On Very Large Scale Integration (Vlsi) Systems, Vol. 18, No. 11, November 2010.
17. Li Xiaoming and Yun Zhao, 2011 “Research on Power Information Encryption Algorithm Based on Composite Chaotic System in Wavelet Transform Domain” ELSEVIER, Procedia Engineering 15 (2011) 2118 – 2122.
18. Carl Landwehr, Dan Boneh, John C. Mitchell, Steven M. Bellovin, Susan Landau and Michael E. Lesk, 2012. “Privacy and Cyber security: The Next 100 Years” Vol. 100, Proceedings of the IEEE.
19. Chung-Ming Ou, 2008 “Design of Block Cipher by Simple Chaotic Functions” IEEE Computational Intelligence Magazine May 2008.
20. Meikang Qiu, Wenzhong Gao, Min Chen, Jian-Wei Niu and Lei Zhang, 2011 “Energy Efficient Security Algorithm for Power Grid Wide Area Monitoring System” IEEE Transactions On Smart Grid, Vol. 2, No. 4, December 2011.
21. Chaturvedi, Ravi Prakash, and Udayan Ghose. "Evaluation of Small Object Detection in Scarcity of Data in the Dataset Using Yolov7." 2023 International Conference on Disruptive Technologies (ICDT). IEEE, 2023.
22. Mishra, A., Gupta, P., & Tewari, P. (2022). Global U-net with amalgamation of inception model and improved kernel variation for MRI brain image segmentation. Multimedia Tools and Applications, 81(16), 23339-23354.
23. Mishra, A., Gupta, P., & Tewari, P. (2023, May). Biomedical Image Segmentation Using Integrated FCM Clustering Modified with Regularized Level Set Method. In 2023 International Conference on Disruptive Technologies (ICDT) (pp. 344-348). IEEE.
24. Chaturvedi, Ravi Prakash, and Udayan Ghose. "A review of small object and movement detection based loss function and optimized technique." Journal of Intelligent Systems 32.1 (2023): 20220324.
25. Chaturvedi, Ravi Prakash & Ghose, Udayan(2023) An effective framework for detecting the object from the video sequences by utilizing deep learning with hybrid technology, Journal of Information and Optimization Sciences, 44:1, 113-126