Acta Scientific COMPUTER SCIENCES

Volume 5 Issue 6 June 2023

Review Article

# Analysis and Study of Cryptographic Algorithm with Context to Cloud Identity and Access Management

**Sudipta Dey[1], Tuhin Sikdar[2] and Tathagata Roy Chowdhury[3]***

*[1]Student, Final Year, Department of Computer Science and Engineering, Brainware University, India*

*[2]Student, Department of Distributed and Mobile Computing, Jadavpur University, India*

*[3]Assistant Professor, Department of Computer Science and Engineering, St Mary's Technical Campus, Kolkata, India*

***Corresponding Author:** Tathagata Roy Chowdhury, Assistant Professor, Department of Computer Science and Engineering, St Mary's Technical Campus, Kolkata, India.

**Received:** March 30, 2023

**Published:** May 23, 2023



## Abstract

Cryptography is one way to ensure that the security and privacy of data provided to the user, as well as the privacy, authentication, integrity, availability, and identification of user data, can be maintained in light of the growing interconnection of computer networks and the sophistication of cyber-attacks. Synchronised key Using a single key for decryption as well as encryption cryptography is a cryptographic approach that guarantees the maximum security and secrecy of data delivered across the communication route. In this paper, we have utilized the cryptographic algorithms and also here we have discussed many concepts which are accurate and proper with the all management. We have specified the cryptographic algorithms, here data of sender is being encrypted and the receiver decrypts the data by using a decryption algorithm in order to get original data, we have discussed the algorithms like, RSA, Diffie Helman, Blowfish and their entire approach, explanation and examples so that the paper will be appeared as good for the researcher in these fields, this papers is utilized to work in Networking Field. This paper is also for them who are working with cryptographic algorithms and all other aspects of network security.

**Keywords:** Cloud; Network; Cryptography; Blowfish; DES; Diffie-Helman; RSA; IAM; Identity Access; Cloud Security; Network Security

## Introduction

In today's world, network security plays an important role in our day-to-day life where network security provides important services mainly maintaining the confidentiality of messages, maintaining integrity of messages, maintaining authentication. In order to deliver the services of network security, cryptography is applied in several areas of network security. For this reason, some cryptographic algorithms have been discussed in this paper [33-35].

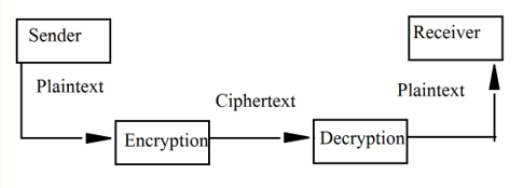


**Figure 1:** Cryptographic Components.

These are the cryptography components (showing on Figure 1.) where sender is in one end and in the other end is Receiver [1,2,12].

## Cryptography

### Basics of cryptography

- It is originated from Greek which refers to "secret writing".
- Actually, cryptography points to the way of transforming data for security purpose

### Encryption and decryption

The procedure of encoding the messages of senders i.e. the plaintext into cipher text is known as encryption and the procedure of reverting back i.e. decoding the cipher text to plaintext is known as decryption [12].

Through encryption algorithm, the original message or data which is also known as plaintext is being transformed to ciphertext. The data of sender is being encrypted and the receiver decrypts the data by using a decryption algorithm in order to get original data. These encryption algorithms are defined as cipher [12].

### Key

This is a number of characters or a set of numbers where the encryption and decryption algorithms (also known as cipher) operate on. Ciphers are divided into two parts:

- Symmetric-key (Secret key)
- Asymmetric-key [3,4].

In case of symmetric-key cryptography, the sender and receiver uses same key for encryption and decryption. But for asymmetric-key cryptography, the encryption and decryption keys are different i.e. the sender uses public key and the receiver uses private key where the sender uses public-key for encryption. Later, the receiver uses private-key for decryption.

So, through the categories of ciphers there are three types of keys. These are:

- Secret-key
- Public-key
- Private-key

Secret-key is used in case of symmetric-key cryptography where the shared key is used by both the sender and receiver for the reason of encryption and decryption.

The key will be known as public-key if the key is shared publicly and used for encryption. So, it is easy to express that the private-key is not shared publicly and used for decryption [19].

### Symmetric-key cryptography

This is a type of cryptography algorithm where the sender and the receiver share same key for the purpose of both encryption and decryption (showing on Figure).

The traditional symmetric-key ciphers can be divided into two categories mainly and those are substitution ciphers and traditional ciphers [12,13].

### Advantages of Symmetric-key cryptography

- The encrypted messages can be reverted back to the plain messages i.e. the decrypted with the help of secret key only.
- Password authentication is used for the authentication of receiver.
- Faster algorithm

### Disadvantages of Symmetric-key cryptography

- Because of sharing secret-key to decrypt, one has to keep an eye on transferring that key in order to save the key from stealing.
- It cannot provide digital signature in any of the encryption.

### Different ciphers

### Substitution cipher

Actually, the substitution cipher refers to the substitution of one symbol with another and the symbols can be characters or numbers. The substitution ciphers are basically divided into two categories; one is known as monoalphabetic cipher and another is known as polyalphabetic cipher [21].

For monoalphabetic cipher, any occurrence of a symbol have same substitute regardless of the position. But for polyalphabetic cipher, each occurrence of a symbol can have different substitutes. Let us demonstrate with examples.

### Example 1

- Plaintext: APPLE
- Ciphertext: ZMRB

### Explanation

Because of being encrypted as M's for both occurrences of P's, this cipher will fall into the category of monoalphabetic cipher.

### Example 2

- Plaintext: HAPPY
- Ciphertext: BERCA

### Explanation

This cipher will might be in the category of polyalphabetic cipher for being encrypted by using different symbols or characters for the occurrences of P's where the first P is encrypted as R and the second P is encrypted as C.

### Shift cipher (Caesar cipher)

The probable simplest monoalphabetic cipher is the shift cipher which is referred as Caesar Cipher sometimes. In this cipher, the encryption algorithm is commonly known as "Shift Key Characters down" having key which is a number. So, in general sense, the "Shift Key Characters up" is referred as the decryption algorithm [21,22].

For an example, let us encrypt a plaintext "NAMASKAR" by using shift cipher with a key of 20 and after that the message will be decrypted in order to have the original plaintext.

- Plaintext: NAMASKAR
- Ciphertext: HUGUMEUL
-

### Explanation

Here, the key is 20. So, the algorithm of encryption is known as "shift 20 characters down". Now, the cipher text will be reverted to plaintext

- Ciphertext: HUGUMEUL
- Plaintext: NAMASKAR

Now, the decryption algorithm is known as "shift 20 characters up".

### Transposition ciphers

In this cipher, the positions of symbols are changed in case of encryption of plaintext [12].

Let us encrypt the message "HELLO BRO" and it shall be decrypted later.

### Encryption

- Let us remove the space which was carried in the message.
- Let us Divide the plaintext into blocks carrying four characters in each block. No extra character is required for now. It shall look like HELL OBRO
- The created ciphertext will look like ELHLOBRO

### Decryption

- Let us divide those characters into blocks again which carries four characters in each
- Let us keep those characters in the previous position which will later look like HELL OBRO
- Let us combine those characters which will after look like HELLO BRO.

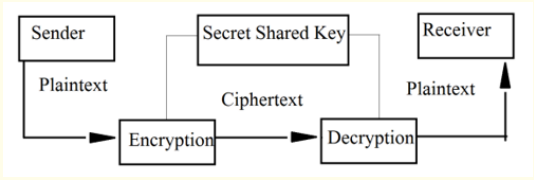


**Figure 2:** Symmetric-key cryptography.

### Asymmetric-key cryptography

In this type of cryptography, two types of keys are used; these are private and public key. Public key is used by the sender for encryption which will be shared publicly. In case of decryption, private key is used by the receiver (showing on Figure) [12,13].

### Advantages of Asymmetric-key cryptography

- No need of exchanging any key
- It allows the acknowledgement of any message which are digitally signed
- Here, the recipient can detect if the message are altered or not

### Disadvantages of Asymmetric-key cryptography

- Slower than symmetric cryptography
- It may hold the longer key than the symmetric-key
- Here, the decryption-key kept secretly

## Different cryptographic algorithms

According to the author, there are several cryptographic algorithms to be followed.

## RSA algorithm

Following steps are implemented to select two keys. These are:

- Private key
- Public key

The algorithm discussed in this way,

- Receiver uses two prime numbers; p and q.
- p and q are multiplied by receiver i.e. n=p × q
- The receiver calculates ⍰ using the values of p and q. The formula implements by the user is ⍰= (p-1) × (q-1)
- The receiver chooses an arbitrary integer e. Then d is calculated (d × e=1 mod ⍰)
- e and n are announced to be public key by the receiver; ϴ and d are kept secret [12,23].

## Diffie-Hellman

Sender and receiver must choose large numbers to calculate $R_1$ and $R_2$ with the following formulae:

$R_1=g^x \bmod p$
$R_2=g^y \bmod p$
[x & y= arbitrary integers] [12,26]

Both sender and receiver share the values of R1 and R2 to each other i.e the sender sends R1 to the receiver and R2 is sent to the sender by the receiver

[x & y are kept secret]

Both the sender and receiver calculate symmetric key K implementing the following formulae:

Sender: K= (R2)x mod p
Receiver: K= $(R_1)^x \bmod p$

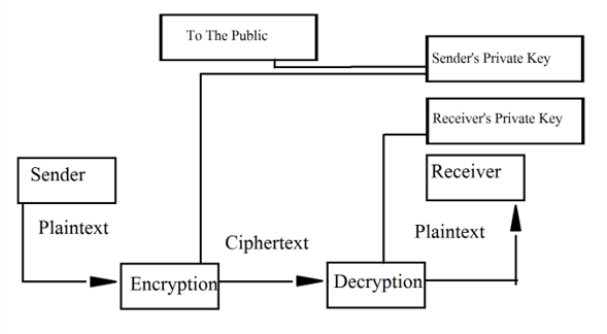


**Figure 3:** Asymmetric-key cryptography.

## Cloud cryptography

## Security-As-A-Cloud-Service

For receiving and transferring data, this is a pay-as-you-go type opportunity which might be cost efficient. For an example, email providers use spam detector to save users from different types of attacks mainly spoofing attack. Another example is HTTPs type website which also ensures everyone whether this website is either reliable or non-reliable (showing on Figure 4) [3].

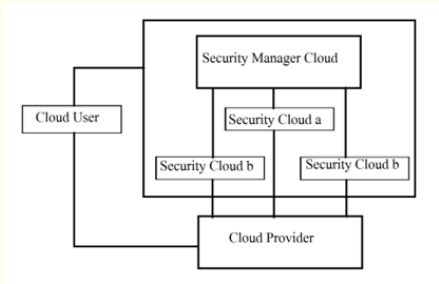


**Figure 4:** Security-As-A-Cloud-Service.

## DES algorithm

The full form of DES is Data Encryption Standard. This algorithm is a symmetric-key algorithm which was published by NIST. For furthermore, this is to say that 64-bit key is used in DES i.e. 64 bits of chunk of data passes through the DES for producing 64 bits of ciphertext. The same key is used for both encryption and decryption which defines the characteristic of symmetric-key algorithm [30].

### Steps

- 64 bit plaintext block should be processed for IP i.e. Initial Permutation
- Then the IP is implemented on plaintext
- Left plaintext and Right plaintext (LPT and RPT) is being created by IP
- LPT and RPT pass encryption process carrying 16 rounds where the encryption process carries five stages:
    - Transformation of key
    - Expansion permutation
    - Permutation (S- Box)
    - Permutation (P-Box)
    - XOR and swap
- LPT and RPT are joined and then a Final permutation i.e. FP is implemented on that combined permutated block of IP

### Blowfish algorithm

This is a symmetric algorithm designed by Bruce Schneier. This is a 64-bit block cipher taking variable-length key. This algorithm contains two parts which are considered as major [19,20].

### Data encryption

It happens on 16-round Feistel iterations having a key-dependent permutation, a key and data-dependent substitution. All encryption happens using XOR gate in addition of 32-bit data [21,22].

### Key expansion and subkeys

Maximum 448 bit keys are converted to subkey arrays in key expansion. The subkeys can be calculated like below:

- With fixed value of hexadecimal digits of pi, the P-array and S-boxes are to be initialized
- First element in P-array is implemented with XOR using the first 32 bits and it continues until all elements in the P-array go under XOR operation
- All zero strings are encrypted as step 1 and step 2
- Following the output from step 3, P1 and P2 are being replaced
- Using modified subkeys, the encryption form of the output is placed
- P3 and P4 are modified through the output of step 5
- The steps are followed until the P-arrays and S-boxes go through the modification.

### AES algorithm

AES consists of linked operations which are in series where some operations replace inputs by some specific output referred as Substitutions and shuffle bits around which are referred as Permutations. So, it can be said that AES is based on the network named as 'Substitution-Permutation network' (showing on Figure 5) [34,35].

Here, the number of rounds depends on the key length; like

- 10 rounds for 128-bit keys
- 12 rounds for 192-bit keys
- 14 rounds for 256-bit keys

The illustration of AES structure is given below:

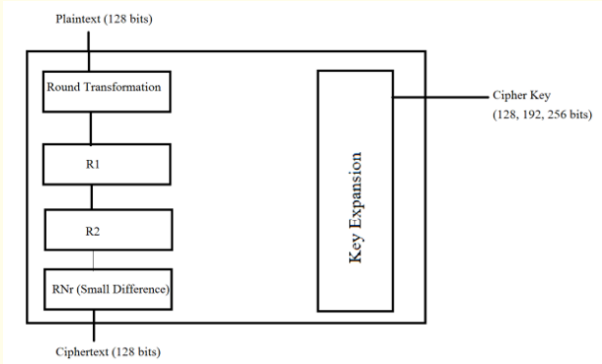


**Figure 5:** AES structure.

### Analysis of AES

- It is supported in software and hardware both.
- No crypto attack has been observed till date.
- It allows 'future-proofing' as AES has built-in flexibility if key length.

### Identity and access management (IAM)

Cloud vendors provide Identity and Access Management (IAM) for securing access to the resources over the internet via cloud. For this reason, AAA is implemented to take the security into the next level [11].

The point to add that AAA is a framework through which can be controlled

- Who is accessed to use the resources?
- What can be accessed?
- What are the users performing?

AAA stands for Authentication, Authorization, Accounting.

### Authentication

The process by which the user can be identified is known as authentication. A user can be authenticated by some credentials like username, password and many more.

### Authorization

Authorization refers to providing the capabilities what a user can be accessed from the network resources after successful authentication.

### Accounting

Accounting mainly refers to monitor a use i.e what a user is doing. In short, it can be said that accounting is nothing but recording the activities of a user by cloud vendors.

## Conclusion

We have utilized the cryptographic algorithms and discussed many concepts which are accurate and proper with the all management, here we have specified the cryptographic algorithms, here data of sender is being encrypted and the receiver decrypts the data by using a decryption algorithm in order to get original data, the algorithms like, RSA, Diffie Hellman, Blowfish and their entire approach, explanation and examples. Also here we have declared different architecture of different algorithms and steps to execute the encryption and Decryption throughout the PT and CT.

This paper also aims to discuss the concepts of Identity and Access Management, which is mainly needed in cloud identity, and its Framework about AAA.

## Acknowledgment

For the guidance of completion of the paper, we should like to express sincere gratitude to Mr. Tathagata Roy Chowdhury who is an Assistant Professor of Computer Science and Engineering in St. Marys Technical Campus, Kolkata.

## Bibliography

1. Khan T., *et al*. "Machine learning (ML)–Centric resource management in cloud computing: A review and future directions". *Journal of Network and Computer Applications* (2022): 103405.

2. Sefati S., *et al*. "Load balancing in cloud computing environment using the Grey wolf optimization algorithm based on the reliability: performance evaluation". *The Journal of Supercomputing* 78.1 (2022): 18-42.

3. Abdulsalam Y S and Hedabou M. "Security and privacy in cloud computing: technical review". *Future Internet* 14.1 (2022): 11.

4. Joseph D., *et al*. "Transitioning organizations to post-quantum cryptography". *Nature* 605.7909 (2022): 237-243.

5. Anusha R., *et al*. "Analysis and comparison of symmetric key cryptographic algorithms on FPGA". In 2022 4th International Conference on Smart Systems and Inventive Technology (ICSSIT) (2022): 293-300.

6. Sohal M and Sharma S. "BDNA-A DNA inspired symmetric key cryptographic technique to secure cloud computing". *Journal of King Saud University-Computer and Information Sciences* 34.1 (2022): 1417-1425.

7. Alwan AH and Kashmar A H. "FCNN Model for Diagnosis and Analysis of Symmetric Key Cryptosystem". *Iraqi Journal For Computer Science and Mathematics* 4.1 (2023): 53-61.

8. William P., *et al*. "Assessment of hybrid cryptographic algorithm for secure sharing of textual and pictorial content". In 2022 International Conference on Electronics and Renewable Systems (ICEARS) (2022): 918-922.

9. Jayaprakash V and Tyagi A K. "Security Optimization of Resource-Constrained Internet of Healthcare Things (IoHT) Devices Using Asymmetric Cryptography for Blockchain Network". In Proceedings of International Conference on Network Security and Blockchain Technology: ICNSBT (2021): 225-236.

10. Thabit F., *et al*. "A Novel Effective Lightweight Homomorphic Cryptographic Algorithm for data security in cloud computing". *International Journal of Intelligent Networks* 3 (2022): 16-30.

11. Sudipta Dey., *et al*. "Analysis and Survey of Eavesdropping on Cloud Platform and Software as a Service with Security". *Acta Scientific Computer Sciences* 5.1 (2023): 130-135.

12. Forouzan B A. "Data communications and networking". Huga Media (2007).

13. Stallings W. "SNMP, SNMPv2, and CMIP: The practical guide to network management". Addison-Wesley Longman Publishing Co., Inc. (1993).

14. Rajasekar V., *et al*. "Introduction to Classical Cryptography". Qu*antum Blockchain: An Emerging Cryptographic Paradigm* (2022): 1-29.

15. Abusukhon A., *et al*. "An authenticated, secure, and mutable multiple-session-keys protocol based on elliptic curve cryptography and text-to-image encryption algorithm". *Concurrency and Computation: Practice and Experience* 34.4 (2022): e6649.

16. Ikematsu Y., *et al*. "Recent progress in the security evaluation of multivariate public-key cryptography". *IET Information Security* (2022).

17. Braeken A. "Public key versus symmetric key cryptography in client–server authentication protocols". *International Journal of Information Security* 21.1 (2022): 103-114.

18. Abu-Faraj M., *et al*. "Increasing the security of transmitted text messages using chaotic key and image key cryptography". *International Journal of Data and Network Science* 7.2 (2023): 809-820.

19. Salmi G N and Siagian F. "Implementation of the data encryption using caesar cipher and vernam cipher methods based on CrypTool2". *Journal of Soft Computing Exploration* 3.2 (2022): 99-104.

20. Diop I and Tall K. "A New hybrid approach of Data Hiding Using LSB Steganography and Caesar cipher and RSA algorithm (S-ccr)". In 2022 International Conference on Computer Communication and Informatics (ICCCI) (2022): 1-4.

21. Hammad R., *et al*. "Implementation of combined steganography and cryptography vigenere cipher, caesar cipher and converting periodic tables for securing secret message". In Journal of Physics: Conference Series 2279.1 (2022): 012006.

22. Popoola D D and Alagbe K. "Secure Message Transmission using Caesar Cipher and Residue Number System" (2022).

23. Sahoo A., *et al*. "Image Encryption Using RSA Algorithm". In Intelligent Systems: Proceedings of ICMIB 2021 (2022): 641-652.

24. Annamalai C. "Factorials and Integers for Applications in Computing and Cryptography" (2022).

25. Gupta C and Reddy NS. "Enhancement of Security of Diffie-Hellman Key Exchange Protocol using RSA Cryptography". In Journal of Physics: Conference Series 2161.1 (2022): 012014.

26. Ametepe A FX., *et al*. "Robust encryption method based on AES-CBC using elliptic curves Diffie–Hellman to secure data in wireless sensor networks". *Wireless Networks* 28.3 (2022): 991-1001.

27. Gebauer L., *et al*. "Secure communication in factories-benchmarking elliptic curve Diffie-Hellman key exchange implementations on an embedded system". In 2022 IEEE 18th International Conference on Factory Communication Systems (WFCS) (2022): 1-4.

28. Peroumal V., *et al*. "FPGA implementation of hybrid asymmetric key-based digital signature and Diffie-Hellman key exchange algorithm for IoT application". *International Journal of Electronic Security and Digital Forensics* 14.5 (2022): 534-546.

29. Mohammed SJ and Taha D B. "Performance Evaluation of RSA, ElGamal, and Paillier Partial Homomorphic Encryption Algorithms". In 2022 International Conference on Computer Science and Software Engineering (CSASE) (2022): 89-94.

30. Reshma RS., *et al*. "Implementing the Comparative Analysis of AES and DES Crypt Algorithm in Cloud Computing". In Computer Networks and Inventive Communication Technologies: Proceedings of Fourth ICCNCT (2021): 325-332.

31. Ajmal A., *et al*. "Cloud computing platform: Performance analysis of prominent cryptographic algorithms". *Concurrency and Computation: Practice and Experience* 34.15 (2022): e6938.

32. Maheswari K U and Sumalatha V. "Cloud Computing based Symmetric Encryption Algorithm (Blueshift)". In 2022 International Conference on Augmented Intelligence and Sustainable Systems (ICAISS) (2022): 904-909.

33. Kadam A K J., *et al*. "Data Storage Security in Cloud Computing Using Aes Algorithm and Md5 Algorithm". *SAMRIDDHI: A Journal of Physical Sciences, Engineering and Technology* 14 (2022): 296-300.

34. Madhavi D., *et al*. "Improving Quality and Correctness of Cloud Data by Implementing AES Algorithm" (2022): 8716.

35. Zhu J. "Research on Secure Storage of Network Data Based on Cloud Computing Technology". *International Journal of Network Security* 24.1 (2022): 68-74.