ISSN 2581 – 3781

AJCSE
ASIAN JOURNAL OF COMPUTER SCIENCE ENGINEERING

Available Online at www.ajcse.info
Asian Journal of Computer Science Engineering 2022;7(2):53-57

RESEARCH ARTICLE

Data Communication Using Cryptography Encryption

K. Suganya, S. Nethra, S. S. Dhanyaa, D. Sudharson

Department of Artificial Intelligence and Data Science, Kumaraguru College of Technology, Coimbatore, Tamil Nadu, India

Received on: 12/02/2022; Revised on: 30/03/2022; Accepted on: 15/04/2022

ABSTRACT

The massive rise of this technology will be critical in the future years. All types of data that exist in the cloud are private to each and every one which can be easily pirated by an attacker when it is sent to the receiver. The desire for honesty, intimacy, solidity, seclusion, and the necessary methods for manipulation are heightened. The below-mentioned article briefly introduces cryptographic methods and a new method of cryptographic algorithms to secure data which improve the security of information that prevents the application in computing of cloud from piracy.

Key words: Cloud computing, Decipher, Encipher

INTRODUCTION

One of the most crucial aspects of today's society is data protection. Cryptography is nothing but writing the text secretly. It is a technique which assures the secrecy of the users' data.[1,2] Cryptography protects a customer's or company's data by switching it to a form that is legible but incomprehensible to unauthorized persons and then turning it again to a format that is readable only with qualified individuals. Figure 1 represents the process of cryptography. An encipher technique that translates the plaintext into another format, called an encipher key ciphertext, and changes the ciphertext into plaintext with the help of identical encipher key or a distinct encipher key depending on methodologies which is being helpful in encryption of data.

TYPES OF CRYPTOGRAPHY

Crypto uses a method of encryption (nothing but turning original data to encrypted data) and decryption (transforming back to original data). There are different types of encipher and decipher, yet the vastly practiced methodologies are listed.

SYMMETRICKEY ENCRYPTION

Using symmetric key cryptographic technique, encryption and decryption of original text can be done using a unique key. Both the clients should know the keys; therefore, they can read or write the data. Figure 2 explains the working of symmetric key Cryptography. Data Encryption Standard, Advanced Encryption Standard, Triple Data Encryption Standard, and other symmetric key algorithms are among them.[3,4]

ASYMMETRIC KEY CRYPTOGRAPHY

Using this approach of cryptographic technique, decryption and encryption of original text can be done using exceptional keys. Public key is a key which is being used to encipher the information and private key is a key which is being used to decipher the information.[5] These keys are distinct from one another. Recipient has the availability only to the private key. Figure 3 explains the working of Asymmetric key Cryptography.

LITERATURE REVIEW

1. "Effective Encipher Schemes in Crypto Improved Security" is offered by Reema Gupta. The study encourages encryption while also examining its limitations and methods.[6] Also addressed various transpositional strategies such as simple columnar and row Route Cipher transposition and so on.[7]
2. "A Revolutionary Rsa Algorithm of Cryptographic Algorithm with High Efficiency for Data Security" is offered by Suyash Verma

Address for correspondence:
D. Sudharson
E-mail: sudharsondorai.ads@kct.ac.in

Figure 1: Process of cryptography

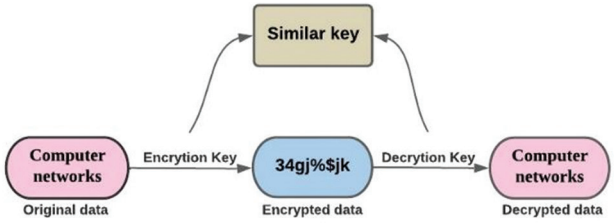

Figure 2: Symmetric key cryptography

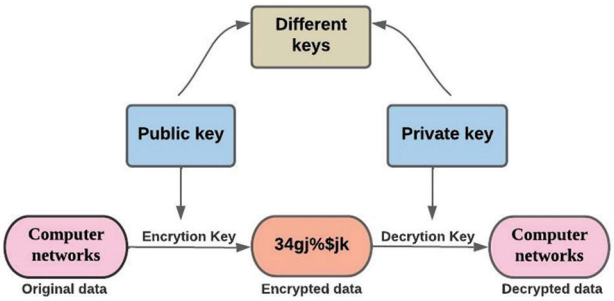

Figure 3: Asymmetric key cryptography

and colleagues. The cryptography technique proposed by him is quicker than the existing one. They arrived at their conclusion by analyzing various simple texts in about the same key (DPSK) method.[8,9]

3. "A Reliable Crypto method for Protecting text messages against Cryptanalytic Attacks and Brute Force."[10] The report explains how Brute force attacks can be protected using the schemes of cryptography.
4. "Cryptography and Network Security," evaluated by Daniel L Calloway, equates and distinguishes studies based on past articles in trend patterns.
5. "A Symmetric Key Cryptographic Algorithm" was postulated by Ayushi. Ayushi launched two kinds of data encryption algorithms, asymmetric and symmetric key.[11] In addition, a dynamic cryptographic technique was developed by her. To convert clear text to encrypted message, she employed keys equal to or larger than 1000, as well as binary and algebraic operations.

PROBLEM STATEMENT

Nowadays, data transmission is not trustworthy. Transmission of data from one server to another server can be sometimes easily cracked or modified.[12] External organizations meddling with transmitting data leads in loss of data or excess of data. Hence, we have tried to find a way to send data in a more secure way.[13]

PROPOSED FRAMEWORK

Symmetric approach

Symmetric key encoding requires minimal runtime, and it is always simple to execute in application scenarios; however, their disadvantage is key's security must be moved in both the clients. This method emphasizes progressing the conventional encryption technology by employing the substitution technique. The first separate character in this suggested technique is transformed into its corresponding ASCII code valuation, as well as further cryptography is accomplished.[14,15]

Encryption methodology

1. ASCII value must be assigned to all the unique characters
2. Hundred must be taken as the key value. ASCII value of the character should be added with the respective key value, and it must be saved in any variable, for example, it can be taken as s1
3. For the value s1 in second step, compute the binary value
4. As the binary values must be a 8 digit number, additional zeroes are added on its left
5. The binary should be reversed for the value in the 4th step
6. The reversed binary numbers should be divided equally into two parts as part1 and Part 2
7. We should calculate 2's complement for both the parts and save it in the complement Part-1 and complement Part-2, accordingly.
   1's complement_ formula=D!=(2^d-1)-D
   Where, D= Positive_Number
   ! represents Complement
   2's complement_formula =D! +i
   Where, D! = 1's complement
   i=1 and it should be added at Least Significant Bit of D!.
8. Complement Part-2 should be joined with complement Part-1
9. Next 2's complement should be calculated for the joined complement parts.

Decimal_Number =D= $B_0 * 2^0 + B_1 * 2^1 + B_2 * 2^2 + \ldots$.
Where, B=binary_digits

10. For the complement parts in 9th step, the hexadecimal code should be calculated.
    Hexadecimal_Number=D/16
    Where, D= Decimal_Number
11. If the hexadecimal code does not have 8 digits add 0 to the left side of the hex code and return it as encrypted data. Figure 4 shows the architecture of Encryption methodology.

Example: -

Imagine the character "G," for instance. Depending on the given technique, the basic methods are obtained.

1. Now take the character G and find the ASCII code for the character which is 71
2. Hundred must be taken as the key value and added to the value of ASCII, S1=71+100 which is 171
3. After that, we must estimate the binary value for 171, which is 10101011
4. Binary value obtained from step 3 already has 8 digits, so we'll continue with Binary as 10101011
5. Binary value in 4th step should be reversed which is 11010101
6. Separate the value of previous steps into two halves as Part 1-1101 and Part 2-0101
7. Next, find the 2's Compliment for Part-1 and Part-2 respectively and save it in complementpart-1: 0011 and complementpart-2: 1011
8. Then, we combine complement Part 2 with complement Part 1, we get 10110011
9. Then, for the binary value acquired in the eighth step, find the 2's complement. 01001101 is the outcome
10. We must find the hexadecimal value for the binary obtained in 9th step which will be f468D
11. To make the hexadecimal value as 8 digits add 0 to the left side and it is transformed into 000f468D.

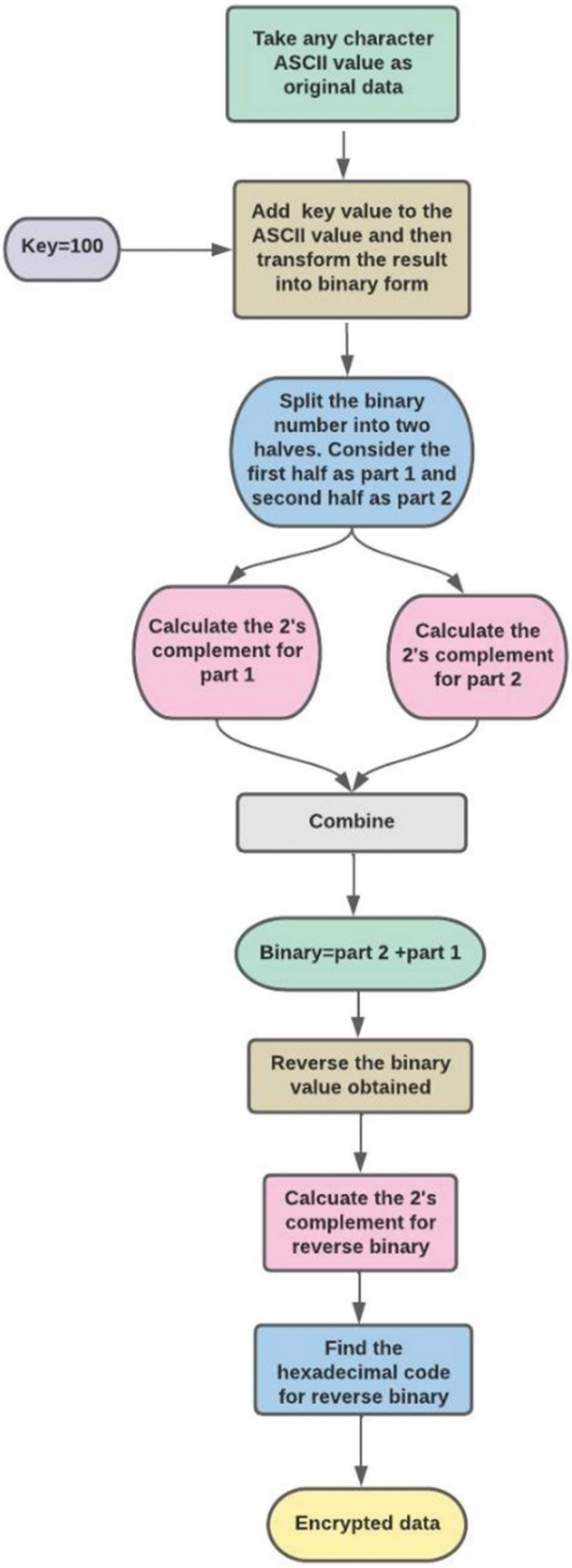

Figure 4: Architecture of encipher technique

Decryption methodology

1. We must transfer the encrypted files to its binary representation
2. Add 0 to the leftmost corner of the binary value to make it as eight digit number if it is not in an appropriate format
3. Generate 2s'complement for the binary value retrieved
4. Slice the binary value into two equivalent parts as Part 1 and Part 2.
5. Then, for Parts 1 and 2, take 2's complement

and save it in the variables complement Part 1 and complement Part 2.
6. Now add the complement Part 2 with the complement Part 1
7. Next the value from the previous step should be reversed
8. Discover American Standard Code for Information Interchange for added complement part of 6th step
9. Hundred is taken as the key value and hence the key is subtracted from value of previous step
10. Now look for one character in the ASCII code. Figure 5 shows the architecture of decryption methodology.

Example: -

Take "000f468D" as Encrypted Data. The steps that precede are generated using specified procedure.

1. Encrypted data should be changed to Binary, which will be 1001101
2. Then we have to format the binary number from 1st step to 8 digits that is 01001101
3. After formatting the number, find the 2's complement for that binary number and the value is 10110011
4. slice the binary from 4th step equally as Part-1: 1011 and Part-2: 0011
5. Next individually find the 2's complement for each part in the previous step and save it in the variables, that is, complement Part-1: 0101 and complement Part-2: 1101.
6. Complement Part 2 is joined with complement Part 1 and the result is 11010101.
7. The result is then reversed as 10101011.
8. The binary number obtained in 7th step is changed into ASCII code which is 171.
9. When we subtract the key which is 100 from the ASCII code in 8th step we get 71 (171–100).
10. From step 9, we obtain the ASCII character value as "G" that is the decrypted data.

RESULTS AND DISCUSSION

The proposed methodology is programmed in Python 3.10.0 for experimental evaluation with PC having the i5 preprocessor and 25 Megabit cache memory with 2.42GHz Intel processor and also having 8GB RAM. The preceding figures show the encrypted and decrypted version of the alphabet "G." Figure 6 shows the output of the process.

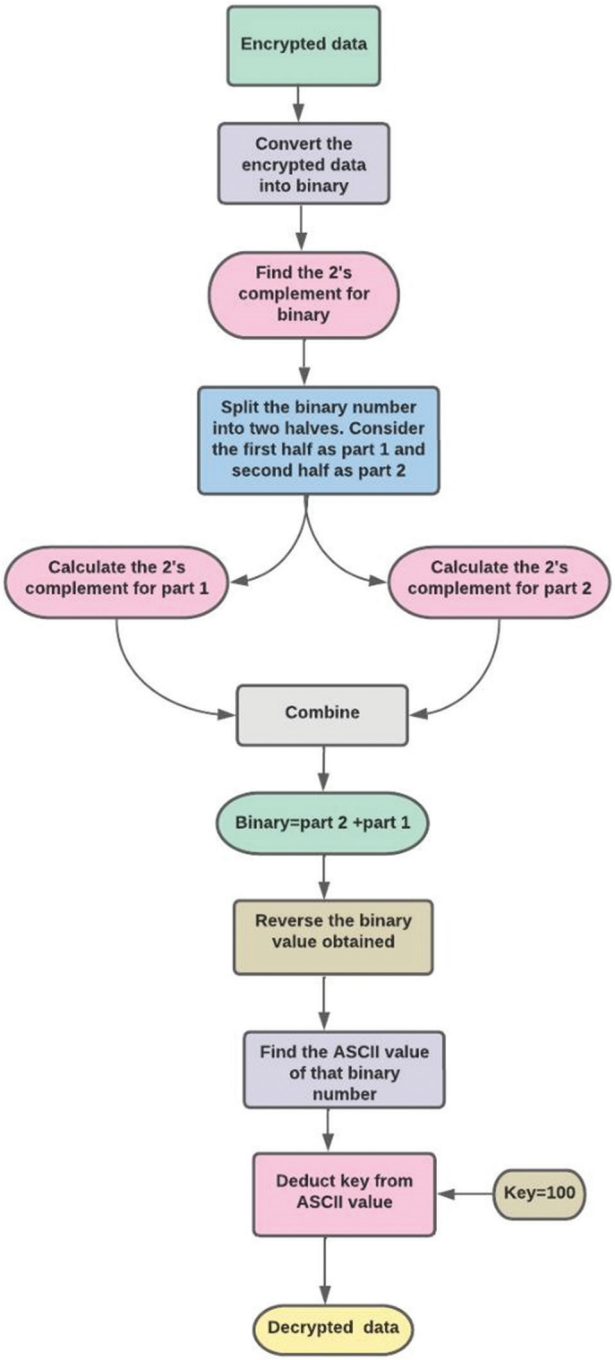

Figure 5: Architecture of decipher technique

```
In [44]: character="G"
         print("Encrypted Text:",encrypt(character,100))

         Encrypted Text: 000f468D

In [45]: print("Decrypted Text:",decrypt(GT,100))

         Decrypted Text: G
```

Figure 6: Output of proposed methodology

CONCLUSION AND FUTUREWORK

To prevent personal information, encryption technology translates actual text into unintelligible textual information. Sometimes, we must exchange some confidential information. Ciphertext is frequently used to protect actual data, also

known as encrypted message, from cybersecurity incidents by altering it to an unintelligible version using a sequence of numbers. A new reliable cryptographic technique is proposed in this paper which is very simple in nature and has the quickest runtime for encryption/decryption. Moreover, the suggested methodology is simple to implement in a real-world problem for the encrypting and decrypting process.

REFERENCES

1. Sudharson D. Performance analysis of enhanced adaboost framework in multifacet medical dataset. NVEO 2021;8:1752-6.
2. Rizvi SW, Singh VK, Khan RA. Fuzzy logic based software reliability quantification framework: Early stage perspective (FLSRQF). Procedia Comput Sci 2016;89:359-68.
3. Sudharson D. A novel machine learning approach for software reliability growth modelling with Pareto distribution function. Soft Comput 2019;23:8379-87.
4. Garousi V, Mäntylä MV. A systematic literature review of literature reviews in software testing. Inform Software Technol 2016;80:195-216.
5. Jacobs IS, Bean CP. Fine particles, thin films and exchange anisotropy. In: Rado G, Suhl H, editors. Magnetism. Vol. 3. New York: Academic Press; 1963. p. 271-350.
6. ArunKumar B. A novel approach for boundary line detection using IOT during tennis matches. Adv Electr Inform Commun Technol 2020;13:243-6.
7. Sudharson D, Fathima SA, Kailas PS, Vaishnavi KS, Darshana S, Bhuvaneshwaran A. Performance Evaluation of Improved Adaboost Framework in Randomized Phases Through Stumps. New Jersey: IEEE Xplore; 2021.
8. Maxwell JC. A Treatise on Electricity and Magnetism. 3rd ed., Vol. 2. Oxford: Clarendon; 1892. p. 68-73.
9. Sudharson D, Rani K. An overview of cloud scheduling algorithms. Vidyabharati Int Interdiscipl Res J 2021:2:78-82.
10. Sudharson D. Improved EM algorithm in software reliability growth models. Int J Powertrains 2020;9: 186-99.
11. Sudharson D. A novel AI and RF tutored student locating system via unsupervised dataset. Turk J Physiother Rehabil 2021;32:882-7.
12. Ayushi A. A symmetric key cryptographic algorithm. Int J Comput Appl 2010;1:181-96.
13. Yuexia Q, Weijie G. The research on reliability optimization of software system based on niche genetic algorithm. AASRI Procedia 2012;1:404-9.
14. Sudharson D, Darshana S, Navin RS, Priyanka K, Ashfia F, Abdulla FM. Self-Reliant Dimensionality Reduction that uses Improved Pareto Distribution PCA Framework. New Jersey: IEEE Xplore; 2021.
15. Mohanty R. Hybrid intelligent systems for predicting software reliability. Appl Soft Comput 2013;13: 189-200.