International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 07 Issue: 06 | June - 2023 SJIF Rating: 8.176 ISSN: 2582-3930

A Comparison of Different Cryptography Algorithms in regards of Data Security

Aviral Jain, Simardeep Singh, Rajdeep Deb, Shery Manchanda, Dr. Vasudha Vashisht

Amity School of Engineering & Technology

AMITY UNIVERSITY, UP

Noida, India

***ABSTRACT*–Organizations all over the world generate a tremendous amount of data on a daily basis since the birth of the World Wide Web and the emergence of ecommerce applications and social networks. The most fundamental difficulty in ensuring secure data transfer over the internet is information security. Network security challenges are also growing more significant as society transitions to the digital information era. It is necessary to safeguard computer and network security, which are crucial challenges. In this paper, we draw a comparison between encryption methods and present an overview of data security and numerous strategies for improving network security, such as cryptography. The rapid advancement of this technology will be critical in the future years. Individuals' data in the cloud is confidential, and it can be hacked by attackers while being shared with the intended receiver. The desire for honesty, privacy, fortification, isolation, and handling processes is increasing. This paper briefly discussed Asymmetric and Symmetric algorithms, their shortcomings and experimented on how fast and secured both the algorithms are. Future scope of this experimentation is immense, more research can be done in developing new algorithms, which provides best of both worlds or research can also be done on perfecting the previous algorithms more and more.**

Keywords: Security, Threats, Cryptography, Encryption, Decryption, Cryptography, Symmetric key , 2's Complement encryption, Data Security, Encryption, Decryption

I INTRODUCTION:

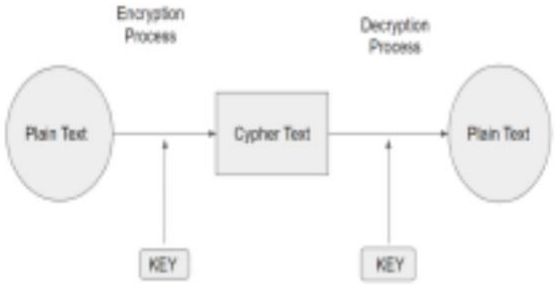
Cryptography means "secret writing" in Greek. Data security is a big worry in today's environment. Cryptography is a way for ensuring data confidentiality. Cryptography protects the privacy of data for an individual or organization by converting the original data to a readable and intelligible format for an unauthorized person and back to the original data for the authorized person. This approach converts

plain text to another format known as cipherText using an encryption key and can also convert ciphertext back to plain text using the same or a different encryption key depending on the technique used to encrypt the data.Because of the rapid development of modern Internet technology and information technology, more individuals, businesses, schools, and government agencies are connecting to the Internet, causing more illegal users to attack and destroy the network at the same time by using fake websites, fake mail, Trojan horses, and backdoor viruses. Computers are the target of network attacks and intrusions, so if the invaders succeed, thousands of network computers will be rendered inoperable.

Furthermore, certain intruders with ulterior objectives target the military and government departments, posing significant challenges to social and national security. Cryptography is short for "Hidden Secrets". Cryptography is the study of systems for secure communication. It is useful for investigating

data security protocols associated with various points of view, such as verification, information classification, non-denial, and information uprightness. The science of writing in secret code is known as cryptography. More broadly, it is concerned with the development and analysis of protocols that thwart attackers; numerous features of information security, such as data secrecy, data integrity, authentication, and non-repudiation, are important to modern cryptography.

The testing problem is how to successfully share scrambled data.



Process of Cryptography

Encoding a message with an unambiguously secure key known only by the transmitting and receiving ends is an important consideration for achieving good security in sensor organizations. The secure exchange of key between sender and recipient is a difficult task in asset crucial sensor arrangement. Clients should scramble information before outsourcing it to a remote distributed storage benefit, and both information security and information access security should be ensured to the point where distributed storage specialist organizations have no capacity to unscramble the information, and when the client needs to pursue a few sections of the entire information, The distributed storage framework will provide availability despite not knowing what the segment of encoded information returned to the client is about. This paper examines various system security and cryptographic methodologies.

II CHARACTERISTICS OF CRYPTOGRAPHY

- Data Security – Secures the plain text
- Data Breaches – Protects from the release of confidential information to the environment
- Authentication and Authorization – Allows only the verified users to have access control of data

III TYPES OF CRYPTOGRAPHY

Cryptography is a process for converting plaintext into ciphertext, also known as encryption, and then back to plaintext, also known as decryption. There are various types of encryption and decryption available, however the most often used cryptographic methods are:

A) SYMMETRIC KEY CRYPTOGRAPHY

A single key is used to encrypt and decrypt the data in this Cryptographic technique. To read/write the data, both clients must know the key. There are various Symmetric key Algorithm approaches, such as DES, 3DES, AES, and others.

B) ASYMMETRIC KEY CRYPTOGRAPHY

This Cryptography technique employs two distinct keys to encrypt and decrypt data. The key used to encrypt the data is known as the Public key, while the key used to decrypt the data is known as the Private key. Both keys are distinct from one another. Only the receiver has access to the Private Key.

IV LITERATURE REVIEW

a) Author I "Efficient Encryption Techniques in Cryptography Better Security Enhancement." The paper promotes encryption and discusses its limitations and approach. We also discussed transpositional approaches such as simple columnar, simple row, and Route Cipher transposition. [7]

b) Author II proposed "A Symmetric Key Cryptographic Algorithm."; She had introduced two types of encryption, Symmetric Key and Asymmetric Key. In addition, she proposed a fast symmetric cryptography technique. She employed keys higher than or equal to 1000 and used binary and mathematical calculations to convert ordinary text to encrypted text.[10]

c) Author III et al. had proposed "A Secure and Fast Approach for Encryption and Decryption of Message Communication"; The authors had talked about cryptography architecture, performance, and other topics. They compared Author III's symmetric technique to their proposed algorithm and discovered that their algorithm was substantially faster. [11]

d) Author IV and their co-author proposed "An Efficient Cryptographic Scheme for Text Message Protection against Brute Force and Cryptanalytic Attacks," The paper describes the cryptographic scheme as well as the protection against Brute Force attacks. The author demonstrates how this technique can be used for important applications. [12]

V SYMMETRIC VS ASYMMETRIC APPROACH

Speed and security choices are the primary distinctions between symmetric and asymmetric encryption. In general, symmetric encryption is faster and easier to use, but it is frequently seen as less safe than asymmetric encryption. But, as previously said, encryption comes down to two factors: key size and the security of the media used to store encryption keys.

Because of the reduced key lengths, symmetric encryption is substantially faster to implement. Because of its higher key lengths and complicated algorithms, asymmetric encryption tends to clog networks. These are the tradeoffs to think about when determining which form of encryption to use. [13]

a) Comparing Speed

	SYMMETRIC		ASYMMETRIC	
KEY SIZE	2048	1024	2048	1024
TIME of Output Generation	3.2 Sec	1.4 Sec	4.9 Sec	2.7 Sec

Table 1: Comparing Speed

b) Comparing Security

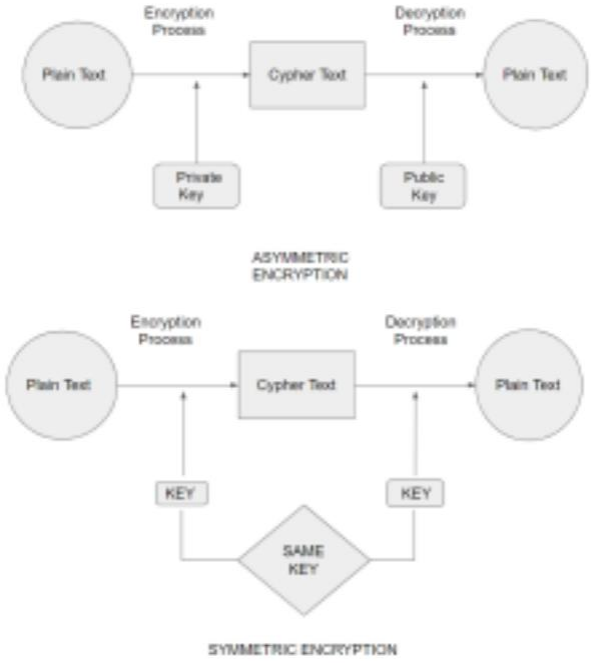
There are only two ways for an attacker to crack an encryption: cryptanalysis and brute force.

Since we are aware of the algorithm AND procedure used to create the encrypted data, we will attempt to determine what the original data was. For instance, if the encrypted data contains a password, we could create a programme that would encrypt each password in a long list of popular passwords before comparing it to the encrypted text. If they matched, we would know the solution. This can be effective in fairly straightforward circumstances but is useless for vast volumes of encrypted data.

	Symmetric	Asymmetric
No of attempts	100	100
Successful Attempts	97	73
Time taken Per Attempt	13 Sec (approx)	25 Sec (approx)

Table 2: Comparing security

Although many encryptions can be broken using supercomputers even without brute force attacks, this method is typically expensive and does not scale. AES 192 bit, on the other hand, would take 500 billion years for the same supercomputer to break if AES 128 bit could be cracked in a second for $10,000.



Cryptanalysis: The two components of cryptology are cryptography, which focuses on developing secret codes, and cryptanalysis, which is concerned with understanding the cryptographic method and cracking those codes. A Cryptanalyst is a person who practices cryptanalysis. By identifying any weak points in the system, it helps us better understand cryptosystems and also improve them. We can then work on the algorithm to produce more secure secret codes. For instance, a cryptanalyst might attempt to extract the plaintext from a ciphertext. It can

assist us in figuring out the plaintext or encryption key. [14]

a) SYMMETRIC APPROACH

Although symmetric key encryption is always simple to implement in practical applications and has a shorter execution time, it has the downside of requiring both clients to transfer their key security. This strategy emphasizes using the Substitution technique to enhance the conventional encryption method[4]. The first character in this suggested technique is translated into its corresponding ASCII code value before the encryption process proceeds.

b) PROPOSED SYMMETRIC KEY ALGORITHM

- ***Encryption Algorithm***

Step 1: Convert a single character to its ASCII value as the first step.

Step 2: Add a key of 100, multiply it by the ASCII value of the character, and then save the result in a variable.

Step 3: Create a binary value using the Step 2 variable.

Step 4: Add 0 to the left side of the integer to get an 8-digit binary number.

Step 5: Reverse the binary result from Step 4 in this part .

Step 6: Separate binary numbers into equal elements 1 and 2.

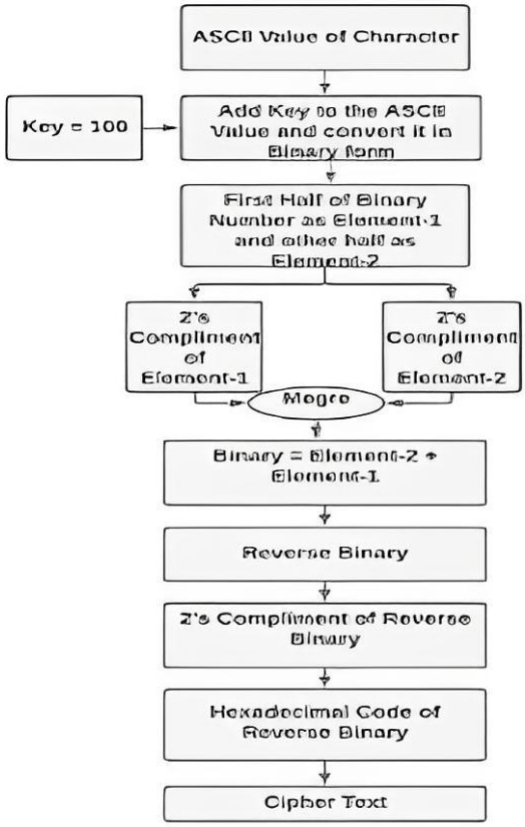
Step 7: In complementElement-1 and complementElement-2, respectively, find the 2's Complement for the two equal parts.

Step 8: Concatenate complement element 2 and complement element 1.

Step 9: Determine the binary's complement, which was obtained in Step 8.

Step 10: From the binary value obtained in Step 9, create the hexadecimal value.

Step 11: Format the Hexadecimal value obtained from Step 10 to have a minimum of



Steps of Encryption Algorithm

eight digits if the code does not already have that many, and then return that value.

- ***Decryption Algorithm***

Step 1: First, convert binary from ciphertext.

Step 2: If the Binary is not already prepared, format it to 8 digits by placing a 0 on the left side.

Step 3: Determine the binary's complement of step two.

Step 4: Divide the binary from Step 2 into elements 1 and 2, respectively.

Step 5: For both equal parts, find the 2's complement and store it in complementElement-1 and complementElement-2, respectively.

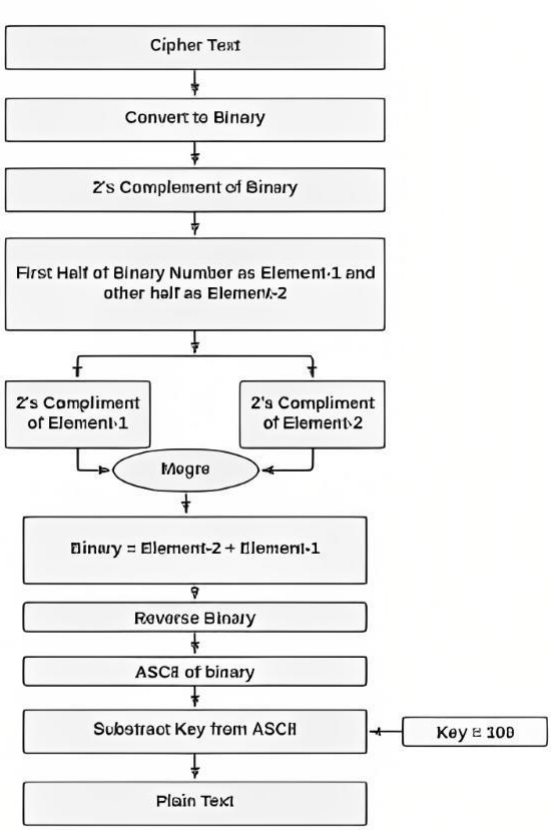
Step 6 : Concatenate the complement elements 2 and 1 in step 6.

Step 7: Reverse the binary result from Step 5

Step 8: Determine the ASCII value of the binary you got in step 6's binary.

Step 9: Deduct the ASCII you obtained in Step 7 from the Key 100.

Convert the ASCII value from Step 8 to its corresponding Character value as a Single Character in Step 10, then return it.



Steps of Decryption Algorithm

1.

EXAMPLE – Take CipherText as "000f4696" for the time being. Now, we shall receive the further stages in accordance with the suggested decryption technique.

We would receive 1001110 after converting CipherText to Binary in Step 1.

Step 2: 01001110 will be the result of formatting the binary number from Step 1 to an 8-digit number.

Step 3: The binary equivalent of two obtained in step two will be 10110010.

Step 4: The binary from Step 4 must now be divided into two equal parts, with element 1 being 1011 and element 2 being 0010.

Step 5: At this point, the complements of each element in Step 4 will be 0101 for Element E and 1110 for E, respectively.

Step 6: The final step is to concatenate the complementElement-2 and complementElement-1, which will result in the value 11100101.

Step 7: The binary we had in Step 6 will now be 10100111 in reverse.

Step 8: The ASCII value of the binary data obtained in Step 7 is 167.

Step 9: We obtain 67 by deducting the key (100) from the value obtained in Step 8. (167-100).

Step 10: The ASCII character value we obtained in Step 9 is "C," which stands for plain text.

VI EXPERIMENTAL OUTCOME

In this experiment we compared both the Symmetric and asymmetric algorithm in detail in terms of security provided by both the algorithms and also on the basis of speed. After taking a large sample of around 100 algorithms each, we can confirm in terms of security asymmetric algorithm is much better than symmetric algorithm and in terms of speed, symmetric algorithms are much faster.

VII CONCLUSION

To protect confidential information, cryptography converts plain text into unintelligible language. On the internet, we must exchange many different sorts of data, some of which may be private. By transforming the original material, which is plain text, into an incomprehensible format using some mathematical combination, cryptography is used to protect the data from unauthorized access. The novel efficient cryptographic algorithm described in this research offers the shortest execution times for both encryption and decryption and is very simple in nature.
Additionally, the proposed algorithm for encryption and decryption is simple to implement in a practical project.

VIII ACKNOWLEDGEMENT

We are grateful to all of those with whom I have had the pleasure to work during the compilation of this research paper. Each of the members of my Dissertation Committee has provided us with extensive personal and professional guidance and taught us a great deal about scientific research. I would especially like to thank Dr. Vasudha Vashisht, our faculty guide during the tenure of this research paper. As our faculty guide and mentor, she has taught us more than we could ever give credit for here. She has guided us through every step of this research paper till the end and this paper would not have been possible without her.

IX REFERENCES

[1] Zhijie Liu Xiaoyao Xie, Member , IEEE ,School of Mathematics and Computer Science and Zhen Wang, Key Laboratory of Information Computing Science of Guizhou Province , Guizhou Normal University Guiyang , China, The Research of Network Security Technologies.

[2] Applying Machine Learning To Predict Symmetric Encryption Algorithm Inputs. A Thesis Presented To The Faculty Of The Computer Science Department California State University Channel Islands In (Partial) Fulfillment Of The Requirements For The Degree Masters Of Science Report Compiled By: Kelly Armstrong Advisor: Dr. Michael Soltys, Mscs Graduate 2019-2021

[3] Shyam Nandan Kumar, "Technique for Security of Multimedia using Neural Network," Paper id-IJRETM-2014-02-05-020, IJRETM, Vol: 02, Issue: 05, pp.1-7. Sep-2014

[4] Daemen, J., and Rijmen, V. "Rijndael: AES-The Advanced Encryption Standard, Springer, Heidelberg, March 2001.

[5] Ritu Pahal, Vikas Kumar,"Ef icient implementation of AES", International journal of advanced research in computer science and software engineering, volume3, issue 7, july2013.

[6] N.Lalitha,P.Manimegalai,V.P.Muthu kumar, M. Santha,"Ef icient data hiding by using AES and advance Hill cipher algorithm ", International journal of research in computer applications and Robotics, volume 2, issue 1 ,January 2014.

[7] IJERT-Cryptographic Algorithm For Enhancing Data Security: A Theoretical Approach. Profile image of IJERT JournalIJERT Journal 2021, International Journal of Engineering Research and Technology (IJERT)

[8] Neha Sharma, Prabhjot and Er. Harpreet Kaur, "A Review of Information Security using Cryptography Technique", International Journal of Advanced Research in Computer Science – Volume 8, No. 4, May 2017 (Special Issue)

[8] Reema Gupta " Ef icient Encryption Techniques In Cryptography Better Security Enhancement" Volume 4, Issue 5, May 2014 ISSN: 2277 128X International Journal of Advanced Research in Computer Science and Software Engineering Research Paper Available online at
"Article: A Symmetric Key Cryptographic Algorithm." International Journal of Computer Applications 2010; 1(14):1–4, DOI: 10.5120/331-502.

[9] Ekta Agrawal, Dr. Parashu Ram Pal, "A Secure and Fast Approach for Encryption and Decryption of Message Communication," International Journal of Engineering Science and Computing. Volume 7 Issue No. 5

[10] A Symmetric Key Cryptographic Algorithm, Ayushi Lecturer, Hindu College of Engineering H.No:438, sec-12, sonipat, Haryana

[11] A Secure and Fast Approach for Encryption and Decryption of Message Communication
E. Agrawal, Dr. Parashu Ram Pal
Published 2017

[12] An Efficient Cryptographic Scheme for Text Message Protection Against Brute Force and Cryptanalytic Attacks
Author links open overlay panelAbhishek Joshi, Mohammad Wazid b, R.H. Goudar, Department of IT,Graphic Era University, Dehradun 248002, India, Research Scholar,CSTAR, IIIT Hyderabad, Department of CNE, Visvesvaraya Technological University, Belgaum 590018

[13] Systematic literature review: comparison study of symmetric key and asymmetric key algorithm: Priasnyomo Prima Santoso et al 2018 IOP Conf. Ser.: Mater. Sci. Eng. 420 012111

[14] 1 of 8 An Overview of Cryptanalysis Research for the Advanced Encryption Standard Alan Kaminsky1, Michael Kurdziel2, Stanisław Radziszowski1 1Rochester Institute of Technology, Rochester, NY 2Harris Corp., RF Communications Div., Rochester, NY ark@cs.rit.edu, mkurdzie@harris.com, spr@cs.rit.edu

[15]A Review Paper On Concepts Of Cryptography And Cryptographic Hash Function, Dr. R.K Gupta Professor, Department of Mathematics, Lovely Professional University, Phagwara