International Journal of Current Advanced Research
ISSN: O: 2319-6475, ISSN: P: 2319-6505, Impact Factor: 6.614
Available Online at www.journalijcar.org
Volume 8; Issue 01(C); January 2019; Page No. 16853-16856
DOI: http://dx.doi.org/10.24327/ijcar.2019.16856.3032

Research Article

HYBRID CRYPTOGRAPHIC ALGORITHM

Mandeep Singh., Simran Babbar., Yankit Kumar and Kritika Malhotra

HMR Institute of Technology and Management, Hamidpur

A R T I C L E I N F O

Article History:
Received 13th October, 2018
Received in revised form 11th November, 2018
Accepted 8th December, 2018
Published online 28th January, 2019

Key words:
RSA Algorithm; AES algorithm; hybrid encryption algorithm; ciphertext; plaintext; information security

A B S T R A C T

The traditional approach towards information security was to use a single encryption algorithm or any well-known cryptographic algorithm. In this paper, a combined encryption algorithm is proposed. That is, the algorithm security is greatly improved through researching and improving some data encryption algorithms, and arranging encryption algorithm in some predefined order. First, write an initial encryption algorithm, second, add in the famous AES algorithm, and then RSA algorithm. Using this hybrid algorithm, the user's information is gradually encrypted, and the algorithm security is greatly enhanced.

INTRODUCTION

The digital age we are currently living in is a password-driven world, where between 4 and 20 characters make the difference in communicating with friends, accessing of data and information or making online transactions. This information is a potential goldmine for those intending to use it for the wrong purpose. Thus, the need for automated tools for protecting files and other information stored on the computer has become evident. The generic name for the collections of tools designed to protect data and to thwart attackers is information security.
To achieve information security, two of the most popular methods are Cryptography and steganography. In this paper we use Cryptography and its algorithms. Cryptography is the process of protecting data by using various methods for converting data into unreadable form, so that only valid users can access data at destination.

Cryptography uses two processes that is encryption and decryption to provide security to data. The encryption is the process of converting plain text (data of given format) into cipher text (data in another format) using an encryption key and the decryption is just the reverse in which the encrypted data is converted back to its original form using a secret key.[23]

Various cryptographic algorithms such as DES, AES, RSA and many more are used for implementing cryptography.

Corresponding author:* **Mandeep Singh
HMR Institute of Technology and Management, Hamidpur

These algorithms are divided into two categories – Symmetric algorithms the one which uses same key for encryption and decryption and Asymmetric algorithms the one which uses two different keys for encryption and decryption.

Symmetric Cryptographic Algorithms also known as private key cryptography is the one in which the secret key is exchanged between the sender and the receiver of the data. The sender encrypts the plain text into cipher text using the key and sends its. The receiver uses the same key to decrypt the cipher text back into plain text.

Asymmetric Cryptographic Algorithms also known as public key cryptography is the one in which one key is used to encrypt the data which is kept private and another key is used to decrypt the data which is kept public. The sender encrypts the plain text into cipher text using any of the two keys and the receiver decrypts the cipher text back into plain text using the opposite key used for encryption.

REVIEW OF LITERATURE

For a strong encryption algorithm, research work by various researchers in the field of encryption and decryption based on different algorithms has been done.[7]

Dr. D.I. George Amalarethinam, J. Sai Geetha, proposed an encryption approach that used RSA algorithm with magic rectangle for encryption. The RSA algorithm was implemented in the traditional way and magic rectangle was used so that there is more level of randomness in the ciphertext values and no repetition is there. But the limitation of this approach was that additional time was required to build the magic rectangle.[24].

Lili Yu, Zhijuan Wang and WeifengWang , proposed a hybrid encryption algorithm that used an initial encryption algorithm, followed by Base64 encryption algorithm and Vigenere encryption algorithm. The initial encryption algorithm used in this approach helped in protection against guessing attacks.[8]
Prof. Vishwanath S Mahalle, Aniket K Shahadepropsed a hybrid encryption algorithm(RSA and AES) to enhance security in cloud computing. It made uploading to cloud , downloading from cloud and sharing more secure as it made use of three keys, public key, private key and secret key.[1]
Chengliang Liang, Ning Ye, Reza Malekian, Ruchuan Wang, proposed a hybrid encryption algorithm that first implemented an improved RSA and then merged AES and improved RSA algorithms to improve security in cloud storage environment.[11]

Design of Hybrid Encryption Algorithm

Initial Encryption Algorithm

This is the first step in the hybrid encryption algorithm. In this algorithm, the ASCII code values of different characters in the plaintext are calculated, so that it cannot be cracked easily. This improves the safety factor.

In general, the plaintext is composed of uppercase letters, lowercase letters, Arabic numbers and other special characters. These different types of characters go through different transformation operations in the initial encryption algorithm as follows:

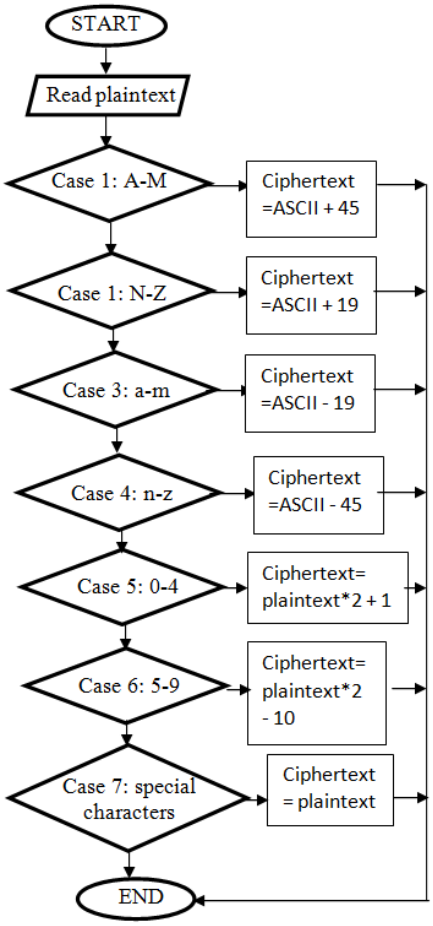

Fig 1 Initial encryption algorithm flowchart

Transformation one: For the upper case letters, in the range A-M in the plaintext, ciphertext is equal to the plaintext ASCII code value plus 45; for the upper case letters, in the range N-Z range, the ciphertext is equal to the plaintext ASCII code value plus 19; for the lowercase letters, in the range a-m, the ciphertext is equal to the plaintext ASCII code value minus 19 ; and for the lowercase letters, in the range n-z, the ciphertext is equal to the plaintext ASCII code value minus 45.[8]

Transformation two: For the Arabic numbers, in the range 0-4 in the plaintext, ciphertext is equal to plaintext multiplied by 2 plus 1; for the Arabic numbers in the range 5-9 in the plaintext, ciphertext is equal to plaintext multiplied by 2 minus 10.

Transformation three: For special characters, the ciphertext is same as the plaintext.

For example, for plaintext “TOmaTO$256”, the ciphertext string after the above steps is “gbZNgb$502”.[8]

Advanced Encryption Standard (AES)

Advanced Encryption Standard is a symmetric algorithm and has been in use since 2001 for providing high level security. [19] It was introduced by NIST (National institute of standard and technology) in 2001 to replace DES (Data encryption standard) to provide security to important documents of US government and then it was implemented for data encryption all around the world. [5] AES uses a block size of 128 bits (fixed) and key of three different sizes 128, 192, 256 bits for providing security to data. These 128 bits are represented using 4x4 matrix. The keys decide the number of rounds such as 10 rounds are used for 128 bit key, 12 rounds for 192 bits key and 14 rounds for 256 bit key.[18]

AES has a particular structure for encrypting the data to provide security. The structure depends on number of rounds.[19] Each round consists of 4 sub processes: -

1. Substitute byte transformation – This is the first stage. Each byte in the state (input data) is substituted with another byte called as sub-byte with the help of non-linear 8-bit substitution box. This S-box is multiplicative inverse over Galois field. [21]
2. Shift row transformation – This is the next step after substitution operation. In it the zeroth row doesn’t go through any transformations. The transformations start from first row. One byte in the first row is shifted circular left. For second row two bytes are shifted circular left. And for the last row three bytes are shifted. The transformations do not change the size of the new state, it remains same as original size i.e. 128 bits. [19]
3. Mix columns transformation - the next step after shift row transformation is mix column transformation in which each column of state matric is mixed. Each column is considered as polynomial over GF (2^8) and then multiplied with fixed polynomial modulo c(x). [19]
4. Add key round transformation – In this last stage both the key and the input data are structured into 4x4 matrix and the subkey is combined with the input data by using bitwise XOR. [19][20]

Rivest-Shamir-Adleman (RSA) Algorithm

RSA is an asymmetric algorithm developed in 1977 by Ron Rivest, Adishamir and Leonard Adleman.[1] Using RSA, the plain text is converted into cipher text by encrypting the text with public key and this text can only be decrypted with receiver’s private key. [4] The main idea of RSA was on prime numbers where it was believed that it is easy to find and multiply large prime numbers but factorization of their product

is difficult. Thus, both the keys in RSA are large prime numbers. The block size for RSA must be less than or equal to $\log_2 n$ where the size of n can be up to 1024 bits.[15][16][17]There are 3 steps in RSA algorithm i.e. key generation, encryption and decryption.

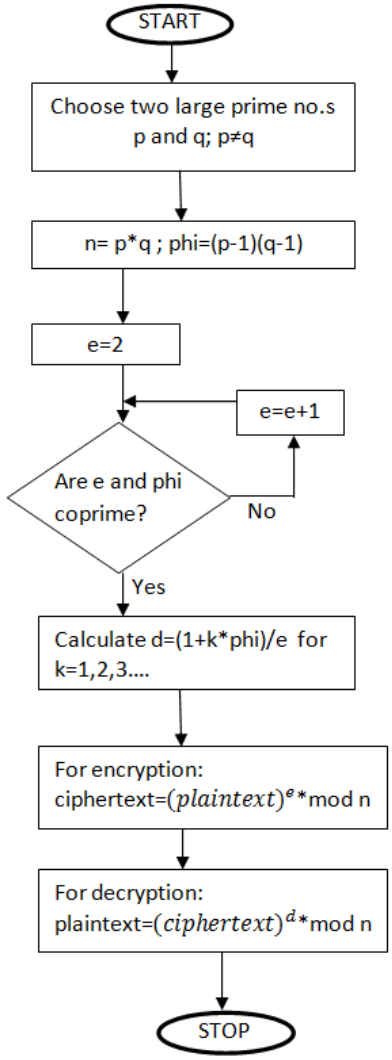

Fig 2 RSA algorithm flowchart

Proposed hybrid encryption algorithm design

The hybrid encryption is an implementation of the initial encryption algorithm, the AES algorithm and the RSA algorithm. This is done in a fixed order: first, the initial encryption algorithm, then the AES algorithm and finally the RSA algorithm.

Take an example of a plaintext string "RaiNBOW270$", after initial encryption algorithm would get converted to string "fMUbtck541$". Second, define the key for AES algorithm. Let key K=1234. On using key K in AES, the string "fMUbtck541$" would get converted to string "hWt2zObHA2TH1ZKFePH3aw==". Then finally use RSA algorithm to convert string "hWt2zObHA2TH1ZKFePH3aw==" to encrypted string "CKQy0PNSjAzZ2pttPLLdz892ogiwWG/C4uvNSV5g4attRQRFGlNn+RupcXXtUXHesWT7p4Bxu0OQtPqnuOLjCA==". The AES algorithm here uses a 128 bit secret key and 1024 bit key is used for RSA encryption and decryption.[10] The three algorithms work independently one after the other for encryption , requiring the user to enter the secret key for AES whereas the keys for RSA are generated automatically ,and in reverse order for decryption.

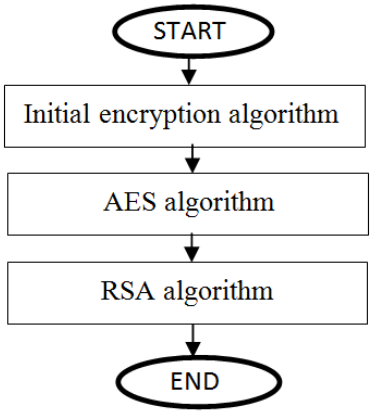

Fig 3 Proposed hybrid encryption algorithm flowchart

RESULTS AND BENEFITS OF HYBRID ENCRYPTION ALGORITHM

1. The proposed hybrid encryption algorithm provides higher lever over security compared to single algorithms.[8]
2. One cannot guess the private key with the help of the public keys generated.[18]
3. The hybrid encryption makes the access of original file by intruders near to impossible.[3]
4. AES provides high speed to hybrid algorithm while RSA provides higher security. Thus this algorithm combines the strengths of both.[11]
5. It is less prone to be influenced by cryptanalysis compared to any single algorithm such as DES.
6. It supports large key sizes.

CONCLUSION

In this era, information encryption algorithm has become an important area of software security. This paper proposed a hybrid algorithm consisting of three parts, the first part is an initial encryption algorithm, and the second and third parts are the traditional AES and RSA algorithms. This hybrid algorithm provides high level of security. It combines the benefits of both symmetric and asymmetric encryption techniques. On this basis, we can add several other well-known encryption algorithms and design a new algorithm. But one major drawback of this algorithm is the high time complexity. Hence this algorithm is not currently used where quick results are required.

References

1. Prof. Vishwanath S. Mahalle, "Implementing RSA encryption algorithm to enhance the data security of cloud in cloud computing", *International journal of pure & applied research in engineering and technology*, 2013, volume 1(8):220-227, ISSN-2319-507X IJPRET.
2. Ms. Thangavel, P. Varalakshmi, MukundMurrali, K. Nithya, "An Enhanced and Secured RSA Key generation scheme", Department of Information Technology, Anna University, Chennai, 2014, Elsevier.
3. Ji Zhang, Tingting Yuan, AES, RSA encryption algorithm hybrid, 2011 Asia- Pacific Youth Conference on Communication, 2011.8.

4. RituTripathi, Sanjay Agrawal, " Critical Analysis of RSA Public Key Cryptosystem", *International Journal of Advanced Research in Computer Science and Software Engineering*, Volume 4, Issue 7, ISSN 2277-128X, July 2014.
5. ElbirtA.J, Yip W., Chetwynd B. , Paar C. "An FPGA-based performance evaluation of the AES block cipher candidate algorithm finalists"′, IEEE Transactions on very Large Scale Integration (VLSI) Systems, Volume: 9 Issue: 4, August 2001.
6. SAHN A, WATES B, "Fuzzy identity-based encryption," Advances in Clyptology-EUROCRYPT. Berlin: Springer-Verlag, 2005:457-473.
7. FengDengguo, "Domestic and abroad research status and development trend of cryptography," Journal of communications, 2002, 05: 18-26.
8. Lili Yu, Zhijuan Wang, Weifeng Wang proposed a hybrid encryption algorithm in 2012 based on a combination of an initial encryption algorithm, Base64 encryption algorithm and Vigenere encryption algorithm. The initial encryption algorithm introduced made it difficult to crack the code.
9. Dr. D.I. George Amalarethinam, J. Sai Geetha, proposed an encryption approach that used RSA algorithm with magic rectangle for encryption.
10. Vishwanath S Mahalle, Aniket K Shahadepropsed a hybrid encryption algorithm (RSA and AES) to enhance security in cloud computing.
11. Chengliang Liang, Ning Ye, Reza Malekian, Ruchuan Wang, proposed a hybrid encryption algorithm that first implemented an improved RSA and then merged AES and improved RSA algorithms to improve security in cloud storage environment.
12. G. Eason, B. Noble and I.N. Sneddon, "On certain integrals of Lipschitz-Hankel type involving products of Bessel functions", Phil Trans. Roy. Soc. London, vol. A247,pp. 529-551, April 1995.(*references*)
13. K. Elissa, "Title of paper if known", unpublished.
14. R. Nicole, "Title of paper with only first word capitalized", J. Name Stand, Abbrev.,in press.
15. JiezhaoPeng, Qi Wu, "Research and Implementation of RSA algorithm in Java",2008.
16. Suli Wang, Ganlai Liu, "File encryption and decryption system based on RSA algorithm", 2011 International Conference on Computational and Information Sciences.
17. Lavanya K. Galla, Venkata Shree Krishna Koganti, Nagarjuna Nuthalapati, "Implementation of RSA", 2016 International Conference on Control, Instrumentation, Communication and Computational Technologies (ICCICCT).
18. Joan Daemen, Vincent Rijmen, "The Design of Rijndael: AES-The Advanced Encryption Standard" in, Springer-Verlag, 2002.
19. Federal Information Processing Standards Publication 197 November 26, 2001 Announcing the Advanced Encryption Standard (AES).
20. AkoMuhamad Abdullah, "Advanced Encryption Standard (AES) Algorithm to Encrypt and Decrypt Data", Cryptography and network security, 2017.
21. TalariBhanuTeja, VootlaHemalatha, KPriyanka, "Encryption And Decryption – Data Security For Cloud Computing – Using Aes Algorithm", SSRG International Journal of Computer Trends and Technology (IJCTT) - Special Issue – April 2017.
22. Nicolas Courtois, Josef Pieprzyk, "Cryptanalysis of Block Ciphers with Overdefined Systems of Equations", pp. 267-287.
23. T. Rajani Devi, "Importance of cryptography in Network Security", 2013 International Conference on Communication Systems and Network Technologies.
24. ShikhaMathur, Vishal Goar, Deepika Gupta, ManojKuri, "Analysis and Design of enhanced RSA algorithm to improve the security", 3rd IEEE International Conference on "Computational Intelligence and Communication Technology (IEEE-CICT 2017).

How to cite this article:

Mandeep Singh., Simran Babbar., Yankit Kumar and Kritika Malhotra (2019) ' Hybrid Cryptographic Algorithm', *International Journal of Current Advanced Research,* 08(01), pp. 16853-16856.
DOI: http://dx.doi.org/10.24327/ijcar.2019.16856.3132

****