Perspective

iMedPub Journals
www.imedpub.com

American Journal of Computer Science and Information Technology
ISSN 2349-3917

2022
Vol.10 No.2:135

An Enhanced Rsa Algorithm for Data Security Using Gaussian Interpolation Formula

Frimpong Twum*

Department of Computer Science, Kwame Nkrumah University of Science and Technology, Kumasi, Ghana

***Corresponding author:** Frimpong Twum, Department of Computer Science, Kwame Nkrumah University of Science and Technology, Kumasi, Ghana, E-mail: twumf@yahoo.co.uk

Received date: January 27, 2022, Manuscript No. IPMCR-22-12443; **Editor assigned date:** January 29, 2022, PreQC No. IPMCR-22-12443 (PQ); **Reviewed date:** February 12, 2022, QC No. IPMCR-22-12443; **Revised date:** February 17, 2022, Manuscript No. IPMCR-22-12443 (R); **Published date:** February 24, 2022, DOI: 10.36648/2349-3917.10.2.135

Citation: Twum F (2022) An Enhanced Rsa Algorithm for Data Security Using Gaussian Interpolation Formula. Am J Compt Sci Inform Technol Vol.10 No.2: 135

Description

Data security is a crucial concern that ought to be managed to help protect vital data. Cryptography is one of the conventional approaches for securing data and is generally considered as a fundamental data security component that provides privacy, integrity, confidentiality and authentication. In this paper a hybrid data security algorithm is proposed by integrating traditional RSA and Gaussian Interpolation formula. The integration raises the security strength of RSA to fifth degree. The Gaussian First Forward Interpolation is used to encrypt the ASCII values of the message after which the traditional RSA is used to encrypt and decrypt the message in the second and third level. The last stage employs Gaussian Backward Interpolation to decrypt the data again. The integration helps to cater for the factorization problem of the traditional RSA. Comparative analysis was performed using four different algorithms; RSA,SRNN, 2-Key pair algorithms and proposed algorithm. It is proven that when the data size is small the encryption and decryption times are lower for the proposed algorithm but higher when the data size is big.

Gaussian Backward Interpolation

A lot of scholars have done various works in-line with data security enhancement. Some aimed at ensuring less execution cost of algorithms while others projected better security of data. To gain a sound understanding, there is therefore the need for review of literature works in a summarized form as presented in this section.

In the author proposed a modified RSA which uses linear order with chosen integer values with a nth modulus similar to the RSA algorithm. Also Wazery and Amin proposed another variant of RSA which uses multiple level scheme to secure data by first employing RSA cryptosystem and then an embedded scheme which uses random placement for selecting data's coordinates when an image is to be considered. This works using dual levels by first scrambling data and then mining to reestablish the data.

According to a Certificate less RSA algorithm by integrating a Kilian-Petrank's RSA with DDH algorithm was also proposed. In their scheme, the private key is the clients secured key. The input value now becomes the user's partial key only to ensure the validity of the scheme. Their scheme had strong security features but was based on the assumption that integrating Kalian with DDH are complex.

Another variant of RSA cryptosystem was also proposed by Budiman et, al, which employed multi-factor RSA scheme. Their scheme worked based on Agrawal-Biswas scheme which scrambles the data and finally unscrambling the ciphertext. Budiman et, al's work was further improved by by using R Prime RSA which is based on large prime numbers which is much secured than traditional RSA which is based on dual prime values. The security of the R Prime RSA is based on the modulus. This means that the higher the modulus the more secured the encryption scheme. This then means if the modulus is less, the security strength becomes weak.

In the works of Bansal and Singh the use of concurrent indexed list of block of characters was also proposed. This has the potential of increasing the encryption and decryption speed of RSA as well as making it compatible with modern industry standards. In the works of Mittal and Aurora a hybrid algorithm that integrates Blowfish and RSA algorithm was proposed. This technique serves both symmetric and asymmetric purposes which makes it efficient.

In Amalarethinam and Leena proposed an Enhanced RSA (ERSA) that injects two additional prime values compared with the traditional RSA. This has the objective of lessening the execution time by breaking the data into units aiming at increasing the security strength of the algorithm. A hybrid algorithm was also proposed by Kaliyamoorthy and Ram lingam that integrates RSA and image steganography. The RSA encrypts the data and the image steganography encapsulates the data from a hacker.

Quasi modified levy flight integrated with RSA was also proposed by Bahraini et.al. The RSA was used to encrypt the data while the Quasi based modified levy flight was used to generate the keys which helped to boost data integrity.

In Khan proposed a hybrid algorithm based on Gulliou-Quisquater scheme and RSA. This aimed at ensuring data

integrity based on the generation of key using the RSA while the Gulliou-Quisquater scheme does the integrity and confidentiality checks.

A three level encryption techniques with the objective of overcoming the use of single key for the encryption and decryption of data through the merge of Advance Encryption Scheme,Data Encryption Standard and RSA was proposed by Subasini and Bushra.

In Mondol and Mahmood proposed a hybrid algorithm utilizing RSA, Blowfish and Secure Hash Algorithm -2. The RSA ensured the authentication of the clients while the confidentiality of the data was secured using Blowfish and the data integrity is secured using Secure Hash Algorithm-2.

Subasini and Bushra proposed a hybrid cryptographic scheme based on RSA, AES and other cryptographic keys. This was meant to secure the safe transfer of data from the client side to the cloud service provider and vice versa.

Mondol and Mahmood proposed the use of RSA scheme to encrypt the data. The RSA is meant for the estimation of different attributes such as Moment Difficulty, Throughput and Area Difficulty. The scrambling is performed at the cloud service provider's end and the encryption at the cloud client's end. In view of the various attempts to help provide algorithms to ensure security of the cloud there is still a gap as can be cited in the works of Kausar Khan.

RSA was proposed in 1977 and is the patent of Ron Rivest, Adi Shamir and Len Adleman, which was published in 1978 at Massachusetts Institute of Technology. RSA as a public cryptographic scheme per literature is known to have a lot of weakness and also with higher execution time. Hence the effort by researchers to propose variant RSA to raise its security strength while reducing execution time.

The Pros of the Hybrid Algorithm

The hybrid algorithm's security strength is based on the conversion of the alphabets in the plaintext to its ASCII values and applying First Forward Gaussian Interpolation Formula on the ASCII values. This helps to make it difficult for any intruder to fish out the plaintext been sent unto the cloud. The result is then acted upon using the traditional RSA scheme. The RSA scheme consists of three stages of Generation of Keys, Encryption and Decryption of the data. Another robustness of the hybrid algorithm depends on second decryption process performed on the decryption from the RSA decoded output. This is attained through the use of the Gaussian Backward Interpolation formula.