# Encryption of Message Using Geometric Progression

Avinay Mehta, Sayan Chakraborty and John Singh K

School of Information Technology & Engineering

Vellore Institute of Technology, Vellore

Email: avinay1165@gmail.com

## Abstract

As in today's world, we store our important data in the form of files in our personal computers and also transfer that data from one person to another. But nowadays the security threats to our data are increasing day by day so we have to transfer our data in such a way that no third party user can access our important information. Therefore to protect our data from the third-party user we need an encryption technique through which we can encrypt our text in the way that no third person can understand the real text behind it. Only the person who has valid key provided by the sender can generate the real message behind that data. As till now, we have come across the many encryption techniques but many of them are not that safe. Therefore we are trying to build a new encryption technique where we actually don't need to encrypt the data within the file we just need to extract some letters from that particular text using the key provided by the sender.

## Introduction

We are in the generation of technology and spend most of our time with computers and hand held devices. In other words we can say that we are in digital world. The digital world makes our life easy and simple. We can easily communicate face to face with the person who is very far from us, purchasing products from online markets, to pay some money to others, everything becomes easy. With the increase of digitization, users of internet have become more. With the increase of use of Internet, threats are also increased. Threats like hacking of account, tracing of somebody transactions etc. These threats are commonly known as cyber threats. The motive of these types of attacks is to steal the information commonly known as active attack and passive attack. To stop these kinds of attacks we have many encryption and description techniques in existence. Encryption is the technique that is used to encrypt or hide the text written by you in the computer. These techniques are mostly used in field where data related to privacy is of high concern like banking, defence, cloud security sharing of messages etc.

## Related Work

In this paper [1] author proposed the security of the high speed data, a throughput resource which is highly efficient AES encryptor/decryptor that works only with logics. Author implements Sbox in which they adopt the method of look-up table that is efficient for Field programmable gate arrays (FPGA) that have 6-input LUTs. A new approach is proposed in which logics are shared between SubBytes and InvSubBytes, which helps to realize InvSubBytes directly with the help of SubBytes having no decomposition into multiplicative inversion. With the help of reordering operation, the data paths of encryption/decryption are unified and they are compressed with some additional multiplexers. Moreover, linear operation between the two nonlinear SubBytes and they are merged into a newly transformed InvMixColumns (NIMC-I). NIMC-I is further optimized so it will reduce the resources and shares the logics with MixColumns.

In this [2] paper presents development of CPA (Chosen Plaintext Attack) protect and RCCA (Replayable Chosen Cipher-text Attack) Attribute Based Encryption (ABE) with some outsourced decryption respectively in generic manner. There is a point to be noted that there are some techniques that are included in construction of RCCA which can implemented in general construction of CCA which secure ABE from the CPA and secure ABE. Authors also have represents the standardized model of construction of CPA secure. There is one more important fact and that there is in verified outsourced decryption in RCCA secure ABE scheme which are already in standardized model that can easily get from the construction of generic RCCA secure. This paper implemented the instantiation of CPA secure. The results which are basis on experiments shows that the existing selective CPA secure system which is compared with other system it is find out that their representation is too dense and has very low cost of computation.

In this paper [3] author tell that security encryption and algorithm in communication, becomes necessary where the time becomes major issue in encryption. For evaluating the performance in RSA algorithm, they have used Short Range Natural Number (SRNN) and 2-Key pair algorithm. Using java library functions the algorithms successfully executed for different file size having 1KB- 150 KB. On the basis of outputs of the experiments that has been conducted in this paper, it has been concluded that the time taken by the SRNN algorithm is less for encryption whereas for decryption RSA algorithm takes less time rather than 2-key pair and SRNN algorithms.

This paper [4] discussed different types of cryptosystems that are being used from decades and their pros and corns. This paper introduced a remarkable concept on elliptic curve technique, its features and its strengths. More importantly how elliptic curve technique is more useful in encryption and decryption of messages. Elliptic curve technique can be used for different cryptography technique like digital signature, authentication etc. There are many real time applications for elliptical curve technique (ECC) such as E-commerce, Secured socket layers applications. Also, for ECC technique low cost implementation technique also and after some tome it will be fixed in commercial security products. This paper provides a detailed description on Elliptical Curve Technique with algorithms for the generation of key for user points that are generated on the Elliptic curve and the decryption of the cipher text as well as plain text message.

In this paper [5] a new colour share generation scheme is being introduced. This scheme uses visual cryptography technique. Here the image which is coloured is encrypted into n number of shares. This paper author uses the algorithm of grey share generation which is implemented using R component and number of multiple grey shares are been created. The resulted shares are joined with B and G component that is used to make the colour sharing which helps to generate the shares in highly secured manner. The resulted secret picture or image has equal size as the size of actual image has. Furthermore the quality of the image is also been maintained.

White box cryptography has [6] its applications in lot of practical problems already. However security can be achieved by placing the part of procedure for creating the white-box implementations secured. But one challenge that researches face is that deriving the methods for white box that does not necessary to have secrecy. To develop one such implementation, one technique is to develop one such strategy that compensates for the loopholes in the current technology. Another technique can be used for developing a satisfactory matched block cipher. There are two techniques Advanced

Encryption Standard (AES) and Data Encryption Standard (DES) which is a representation for providing the good security and efficient implementation for Black Box security on various platforms. It can also be achieved from the execution of the security of black box; if there is an outline of a block cipher have an aim to give this kind of implementation.

This paper analyzes the execution of BRA and AES algorithms for encrypting and decrypting the files. It can be concluded from the analyzation that the execution of 'Byte Rotational Algorithm' is far better than AES algorithm. In case of encrypting the message, AES takes five to thirteen percent more time for execution in comparison with byte rotational algorithm. Similar is with the decrypting the message also where AES takes 'five to fourteen' percent of more time. For encrypting the picture AES takes 'five to seventeen' percent more time and for decrypting the picture it takes 'four to sixteen' percent more time than BRA algorithm. So, it is concluded from the paper that when compared to AES, BRA algorithm consumes very less time and thus offers good performance for encryption and decryption of data. We can also implement other new hybrid models, with reduced time and improve network security for encryption and decryption of data.

This paper proposes [8] and implements the sharing of images in a secured manner over internet with the help of "Transposition Based Symmetric encryption and decryption". We can compute the efficacy of this technique in terms of the "index correlation "and "entropy for different rules of permutation". The most efficient permutation is find which has less index of correlation and powerful entropy.

In this "KeePass" 2.30 sign in authentication [9] takes place four times of 'SHA-256' and by default there is 6000 AES algorithm rounds that will increase the cracking time of password. The size of the Key is 256 bytes, which will make the hack of password almost not possible. It is due to the reason of secured AES algorithm. KeePass 2.30 has excellent response. The experiments that is made on this paper, it has been concluded that the length of the passwords must be more than 6 bytes or more. It can also be possible to increase the rounds for encrypting the passwords that makes to crack the password very tedious.

# Proposed Methodology

Here we are using geometric progression (G.P) to share the secret message between sender and receiver.

Here 3 keys will be generated key(a,r,n) using Diffie Hellman Algorithm:-

where

a=first letter position

r=difference of letter

n=number of letters

Let key= (6, 2, 4)

Where

6 is the first position of the letter

2 is the common difference between the position of the letter

4 is the total number of letters

Therefore using G.P formula for sequence generation:-

$\{a,ar,ar^2,ar^3,--------,ar^n-1\}$

So by applying the formula receiver will generate there 4 terms using the key a=6, r=2, n=4 are:-

6,12,24,48 will be the position of the result.

# Implementation

The technique is implemented using JAVA programming.

Algorithm:-

Step 1 :First choose 2 prime numbers g and p where g is primitive root of p.

Step 2 : First user choose a random secret no(**x**) and computes $\mathbf{g^x}$ *mod* p , let's call it X. First user sends X to Second user.

Step 3 : Second user choose a random secret no(**y**) and computes $g^y$ *mod* p**,** let's call it Y**.** Second user sends Y to First user.

Step 4 : Now First user computes $S\_X = Y^x \bmod p$

Step 5 : Second user computes $S\_Y = X^y \bmod p$

Step 6 : If S_X=S_Y then First user and Second user can agree for future communication.

Step 7: If above condition satisfies then Construct an object of File Reader class for getting the path of a file.

Step 8: Storing the text into an array a[] that we fetch from the file.

Step 9: Now apply the program of geometric progression up to n values.

Step 10:Now the values generated by the geometric progression will fetch the data stored in the particular array location a[].

# Conclusion

In this paper we have implemented a new cryptographic encryption technique using geometric progression through JAVA. We are getting our encrypted data from file messages. The technique is very simple and it contains all meaningful data. If any intruder wants to decrypt the file then it might possible that he/she would get some meaningful data. But it is not necessary that it is the actual data that is send by the sender and due to this technique it will make the intruder more tedious and confused to crack the message or data which is sender is sending to the receiver.

# References


[1] Lijuan Li, Shuguo Li, "High Throughput AES Encryption/Decryption with Efficient Reordering and Merging Techniques" In proceedings of IEEE International Conference on Field Programmable Logic And Applications, pp 1-4,2017.

[2] Xianping Mao, Junzuo Lai, Qixiang Mei, kefei Chen, Jian Weng, "Generic and Efficient Constructions of Attribute-Based Encryption with Verifiable Outsourced Decryption", In proceedings of IEEE Transactions on Dependable and Secure Computing, pp 533-546, Vol 13, Issue 5,2016.

[3] Sarika Y. Bonde, U.S.Bhadade,"Analysis of Encryption Algorithms RSA, SRNN and 2 key pair for Information Security " In proceedings of IEEE International Conference on Computing, Communication, Control and Automation, pp 1-5,2017.

[4] Madhira Srinivas, Sammulal Porika, "Encryption and Decryption Using Elliptic Curves for Public Key Cryptosystems " In proceedings of IEEE International Conference on Intelligent Computing and Control Systems, pp 1300-1303,2017.

[5] Trupti Patel, Rohit Srivastava,"A New Technique for colour Share Generation using Visual Cryptography", In proceedings of IEEE International Conference on Research in Intelligent and Computing in Engineering, pp 1-4, 2016.

[6] Wil Michiels, "Opportunities in White-Box Cryptography ", In proceedings of IEEE Security and Privacy, PP 64-67, Vol-8, No 1,2010.

[7] Punam V.Maitri, Dattatray S.Waghole, Vivek S. Deshpande, “Low Latency for File Encryption and Decryption Using BRA Algorithm in Network Security”, In proceedings of IEEE International Conference on Pervasive Computing (ICPC), pp 1-4,2015.

[8] S. Emalda Roslin, N.M. Nandhitha, Anita Dainel, “Transposition Based Symmetric Encryption and Decryption Technique for Secured Image Transmission through Internet”, In proceedings of IEEE International Conference on Circuits, Power and Computing Technologies [ICCPCT-2014], pp 1578-1583,2015.

[9] Hengwei Zhang, Jingxin Hong, Jun Hu, “Analysis of Encryption mechanism in KeePass Password safe 2.30”, In proceedings of IEEE International Conference on Anti-counterfeiting, Security, and Identification (ASID), pp 43-46,2016.