International Journal of Applied Engineering Research ISSN 0973-4562 Volume 11, Number 1 (2016) pp 681-684

The Complex Key Cryptosystem

D. Negi
Assistant Professor, Gyani Inder Singh Institute of Professional Studies, Dehradun, Uttarakhand, India.
E-mail: dsingh.negi23@gmail.com

A. Negi
Associate Professor, Department of Computer Science and Engineering, G.B. Pant Engineering College, Pauri, uttarakhand, India.
E-mail: ashish.ne@gmail.com

S. Agarwal
Assistant Professor, Department of Computer Science and Engineering, J.S.S Academy of Technical Education, Nodia, India.

Abstract
Cryptography is an effective way of protecting sensitive information transmitted through network communication paths. It is the science of protecting information by encoding and decoding of input message. In this paper we present an effective two tier complex key encryption/decryption model using dynamical system and fractal sets.

Keywords: Fractal, Mandelbrot set, cryptography, security.

Introduction

The Mandelbrot set is the most famous of all fractals. It is easy to generate on a computer and full of fascinatingly beautiful detail. B. Mandelbrot, scientist and mathematician at IBM, is often characterized as the father of fractal geometry [1]. Mandelbrot coined the word fractal in the late 1970s. The most amazing thing about fractals is the variety of their applications. Besides theory, they were used to compress data in the Encarta Encyclopedia [1] and to create realistic landscapes in several movies like Star Trek. Earlier, French mathematician Gaston Julia (1893-1978) introduced a set named Julia set [2]. The set of points with chaotic orbits is called the *Julia set* for a given function. The connection between the Mandelbrot set and the Julia set is that each point c in the Mandelbrot set specifies the geometric structure of the corresponding Julia set [3]. *Thus the Mandelbrot set is the collection of all points in the complex $c-$ plane where the orbit of the iterations of $f(z_n)$ is bounded.*

The primary need of an effective communication system is to provide transmission of information in a secure manner. Cryptography is an effective solution to securing communications over open networks. Encryptions, digital signatures, password-based user authentications are some of the most basic cryptographic techniques for securing communications [4]. However, for many "fancier" applications, the basic cryptographic techniques are no longer adequate. The encryption technique now days are modernized with different algorithms implementing truing of plaintext information into unintelligible format ciphers text. In this paper we present a new and effective encryption technique based on fractal encryption algorithm which uses the famous Mandelbrot and Julia set fractal to generate the encryption key. This proposed fractal encryption algorithm generate efficient random expanded key by using the Julia fractal instead of using a fixed convention rule. The transmission of massage over the network is a critical task requires users to share information in a way that other can't decipher the flow of information. Also, the keys required for encryption and decryption must be randomized and randomly generated from the changing data bits. The algorithm proposed in this paper satisfy the above two criteria to some extent.

Thus we ensure that the data packets are bounded to an group rather than particular node. Thus the data can be addressed by the area name.

Preliminaries

Mandelbrot Set

Mandelbrot set M for the quadratic $Q_c(z) = z^n + c$ is defined as the collection of all $c \in C$ for which the orbit of point 0 is bounded, that is,

$$M = \left\{ c \in C : \left\{ Q_c^n(0) \right\}; \quad n = 0,1,2,3...is\,bounded \right\}$$

we choose the initial point 0, as 0 is the only critical point of Q_c [5].

Julia Set

The set of points K whose orbits are bounded under the iteration function of $Q_c(z)$ is called the Julia set. We choose the initial point 0, as 0 is the only critical point of $Q_c(z)$ [5].

Public Key (Asymmetric Cryptography)

The security is the process of protecting data from unauthorized access, destruction, modification etc. This can done by either be a symmetrical key (both encrypt and decrypt use the same key) or asymmetrical (encrypt and

decrypt keys are different) the RSA encryption that is based on uses and asymmetrical key, in this technique the public key is significantly different from the decryption key. In the case of RSA encryption algorithm, it uses very large prime numbers to generate the public key and private key, which makes it impractical to use.

In this paper we present a new encryption technique based on the complex number rather than the prime numbers, we uses these complex number to make both private key and public key, the idea comes from the chaotic nature of fractals [6], we have use the chaotic nature of fractals to encrypt and decrypt the message respectively. Key size generally determines the number of guesses that an attacker would need to make in order to find the key e.g. brute force; it determines the chance and feasibility of a collision attack. But using the fractal key, the exchange key space depends on size of the keys, which extend the key space, shrink the key size and make more complex.

The existing cryptographic system uses two keys, a public-key which is known to everyone and a private-key or secret key known only to the recipient of the massage [7]. It is to mention that the public- key and private key both are related in such a way that only the public-key can be used to encrypt messages and only the corresponding private-key can be used to decrypt them, moreover it is very difficult or impossible to deduce the private key if anyone know the public-key [8]. As an example if we have 128 bit key, there are 2^{128} possible key values [9]. In the proposed model, we have implemented the two dimensional complex space (see fig. 2) rather than real space, with 60 bit key so there are 2^{60} possible key values. Another example is the Diffie Hallman key space (DH key space) protocol which depends on large prime numbers. The DH Key space for 128 bit is limited by how many primes exist in the finite field of $\boldsymbol{Z_p}$, where $\boldsymbol{p}$ is the largest prime that can be represented by 128 bit value [9]. Therefore, the DH Key space is considerably smaller than the Fractal key space, see [9] [Table 1].

Diffie-Hellman Key Exchange

The Diffie and Hellman first introduced public–key algorithm in 1976 in the seminal paper that defined public key cryptography, The purpose of the algorithm is to enable two users to exchange a secret key securely that then can be used for subsequent encryption of massages. The Diffie-Hellman algorithm depends for its effectiveness on the difficulty of computing discrete algorithm [9].

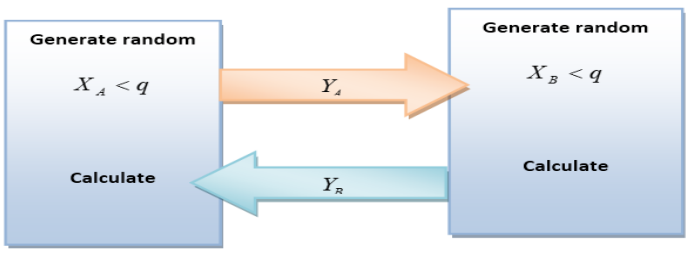

Figure 1: Diffie-Hellman Key Exchange.

Key Exchange Protocol Based on the Fractals

Recently Alia [9] introduced study the key exchange protocol based on the Mandelbrot and Julia sets in their study they explore utilizing fractals strong properties and designed a new protocol. Their encryption technique depends on the number of iterations which convert the value of c in the Mandelbrot set and starting value of z in Julia set further adding the value of e and d in the iteration process, see [10].

Proposed Complex Key Cryptosystem

An algorithm to present a new approach for complex encryption and decryption technique base on fixed point iteration. Such type of encryption technique gives higher level of security as the private function & private key. The chaotic nature of the fractal functions ensures the security of the proposed protocol [11]. The purpose to choose Mandelbrot set is due to the fact that the Mandelbrot set consists of infinite unique connected Julia sets, which gives the freedom to choose random public key. The proposed encryption algorithm consists of the following process as shown in figure below.

Sender Side

Step1: Sender generates a public- key c from connected Julia set.

Step2: Sender generates private-key d by using public-key c & function $f(n)$.

Step3: Message is encrypted with private key $f_e(n) = f(msg)$.

Step4**:** Public key and encrypted Message are send to the receiver.

Receiver Side

Step1: Receiver receives a public- key c and encrypted message $f_e(n)$.

Step2: Receiver generates private-key e by using public-key c & function $f(n)$.

Step3**:** Encrypted message is decrypted using the private-key $f'(n) = f'(msg)$

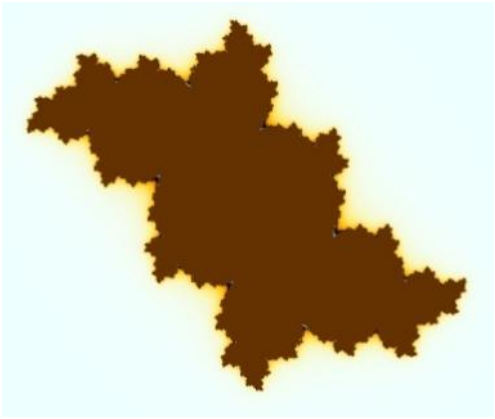

Figure 2: Connected Julia Set For $(-0.1375, 0.66125\,\boldsymbol{i})$

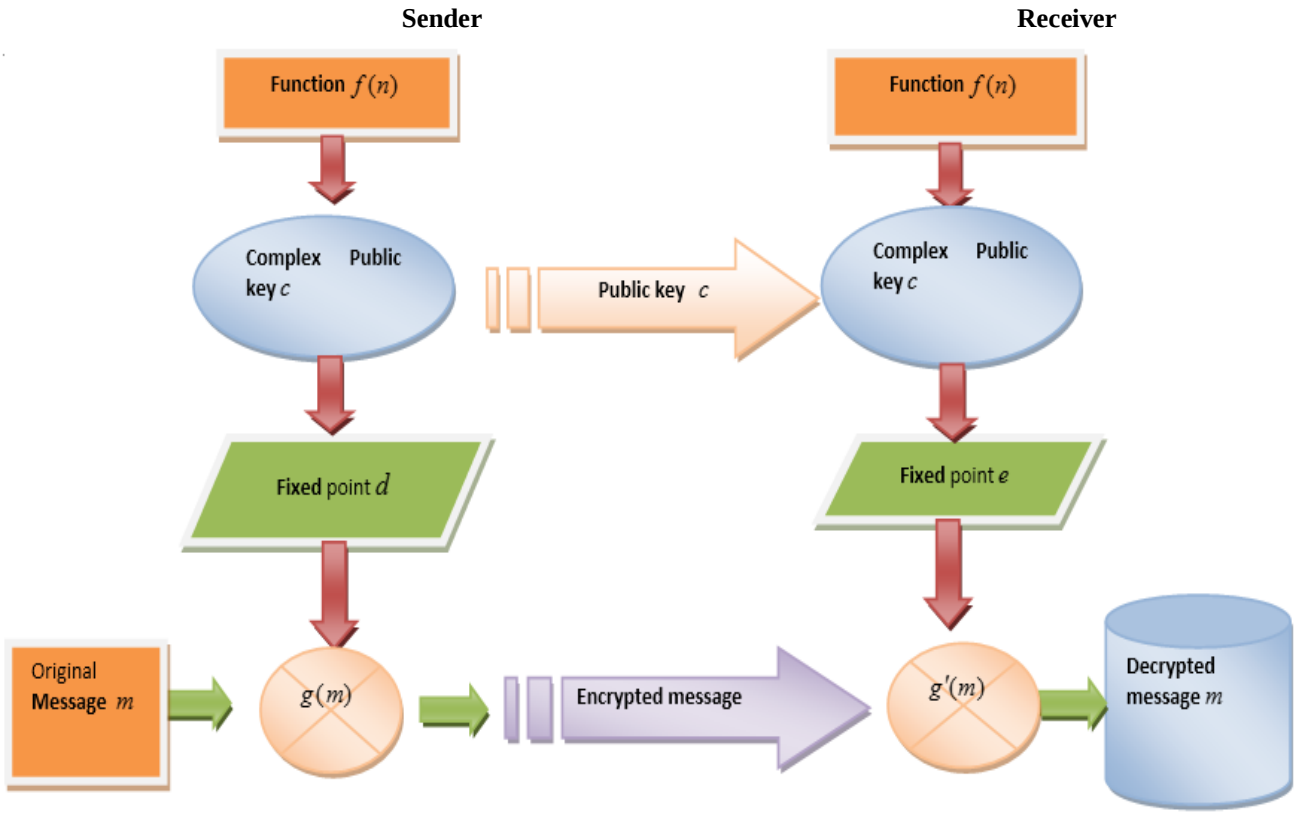

Figure 3: Proposed Model

Encryption Process

Encryption is a way, even if unauthorized person mange to access the encrypted data, all they find is nothing but streams of unintelligent, alphanumerical characters. In term of encryption process, the algorithm consists of combination of public key and function infrastructure. The first step in this proposed method is to generate the complex public-key, say c, a parameter of connected Julia set corresponding to the Mandelbrot set defined by the function $f(n)$. As all corresponding Julia set inside the Mandelbrot set are connected [4], we choose a random connected Julia set. The private key is initialized by the fixed point of the iteration for $f(n)$, say $\boldsymbol{d}$. Finally the massage is encrypted using the private key and transmitted.

Decryption Process

The decryption process involves converting the encrypted data back to its original form for the receiver's understanding. The same process is performed at the

beginning of encryption and decryption process as described in the encryption part at the sender side to generate the same private position at the receiver side to eliminate the key from the cipher text. The proposed decryption algorithm decrypts the encrypted message using the private key e. The private key e (at the receiver end) is generated by iterating the function $f(n)$ and the public key c. Finally the message is decrypted on applying this private-key on encrypted message. The detailed working process is given in Table 1.

Table 1: Example Of Fractals Based Key Exchange Protocol.

Description	Sender	Receiver
Function	$f(n)$	$f(n)$
Generate a public key (c)	-0.1375 , + 0.6125i	-0.1375 , + 0.6125i
Generate private key (d)	-0.2429, +0.4118i	-0.2429, +0.4118i
Encrypt the message $f(n) = f(msg)OR(d).$	$f(n) = f(msg)$ -0.2429, +0.4118i	$f(n) = f_e(msg)$ -0.2429, +0.4118i
Encrypted message	1.0e+002,1.0876 + 0.0041i 0.9676 + 0.0041i 1.1476 + 0.0041i, 1.1476 + 0.0041i 0.9676 + 0.0041i 1.0276 + 0.0041i, 1.0076 + 0.0041i	1.0e+002,1.0876 + 0.0041i 0.9676 + 0.0041i 1.1476 + 0.0041i, 1.1476 + 0.0041i 0.9676 + 0.0041i 1.0276 + 0.0041i, 1.0076 + 0.0041i
Type of message	Encrypted Message $f_e(msg)$	Decrypted message $f_e(msg)$

Conclusion and Remarks

The conventional cryptography technique is no longer adequate. Hence, the need of the hour is an efficient but simple, encryption and decryption algorithm for encrypting any kind of data. Using fractal with cryptography gives a larger set of key values as compared to other algorithms based on prime values existed for a given key size. Also, the key required for encryption and decryption must be randomized and randomly generated. In this paper we have introduced a new system using complex keys to encrypt and decrypt algorithm works on the two tier security locking system, public/private key as well as the information. Without knowing two of them, it is impossible to decrypt the message. There are infinite functions for the infinite c values in complex plane; hence, the guessing domain for the attacker is also increased to infinite. The purposed algorithm is based on complex key numbers and fixed point iterations which are possible due to the intrinsic connection between the Mandelbrot and Julia fractal sets. Therefore, it is a good alternative for applications due to its high level of security.

References

[1] Peitgen, H. (1986). 0. and PH Richter, The Beauty of Fractals: Springer Verlag, Berlin.
[2] Peitgen, H.O., Jürgens, H., & Saupe, D. (2006). Chaos and fractals: new frontiers of science: Springer Science & Business Med
[3] Barnsley, M. F. (2014). Fractals everywhere: Academic press.
[4] Morabito, M., & Devaney, R. L. (2008). Limiting Julia sets for singularly perturbed rational maps. International Journal of Bifurcation and Chaos, 18(10), 3175-3181
[5] Chauhan, Y. S., Rana, R., & Negi, A. (2010). Mandel-Bar Sets of Inverse Complex Function. International Journal of Computer Applications, 9(2), 17-24.
[6] Zakeri, S. (2006). On biaccessible points of the Mandelbrot set. Proceedings of the American Mathematical Society, 134(8), 2239-2250.
[7] Menezes, A. J., Van Oorschot, P. C., & Vanstone, S. A. (1996). Handbook of applied cryptography: CRC press.
[8] Thomas, T. M., & Stoddard, D. (2011). Network security first-step: Cisco Press.
[9] Alia, M. A., & Samsudin, A. (2007). New Key Exchange Protocol Based on Mandelbrot and Julia Fractal Sets. International Journal of Computer Science and Network Security (IJCSNS), 7(2), 302-307
[10] Patrzalek, E. (2006). Fractals: Useful Beauty General Introduction to Fractal Geometry. Stan Ackermans Institute, Centre for User-System Interaction, Eindhoven University of Technology.
[11] Stallings, W. (2007). Network security essentials: applications and standards: Pearson Education India.