American Journal of Educational Research, 2016, Vol. 4, No. 13, 931-936
Available online at http://pubs.sciepub.com/education/4/13/3

DOI:10.12691/education-4-13-3

Encryption Using Contractive Functions

Asha Rani[1,*], Kumari Jyoti[1], Naveen Kumar Antil[2]

[1]Department of Mathematics, SRM University, Haryana, Sonepat- 131001, India
[2]CITD, Rakuten India, Bangalore- 560054, India
*Corresponding author: asha.dahiya27@gmail.com

Abstract In this paper we introduce a fresh encrypting strategy. Our encryption scheme is based on the concept of contractive functions in a Banach space. The algorithm uses two different concepts of mathematics: contraction principle, unique prime factorisation theorem. The mixture of these two concepts is beautiful and it promises a high level of security with an easy to learn mechanism.

Keywords: *encryptions, contractive functions, banach contractive principle, unique factoriation theorem*

Cite This Article: Asha Rani, Kumari Jyoti, and Naveen Kumar Antil, "Encryption Using Contractive Functions." *American Journal of Educational Research*, vol. 4, no. 13 (2016): 931-936. doi: 10.12691/education-4-13-3.

1. Introduction

The data that can be read and understood without any special measures is called a plaintext or cleartext. A method of disguising the plaintext in such a way that hides its substance is called an encryption. Encryption of a plaintext results into unreadable gibberish which is called ciphertext. We use encryption to ensure that information is hidden from anyone for whom it is not intended, even those who can see the encrypted data. The process of reverting ciphertext to its original plaintext is called decryption.

In past, many techniques have been used for encryption in order to maintain secrecy. Julius Ceaser used D in the place of A, E in place of B, and so on in his messages, only the person knowing the 'shifting by three places' hence can decode the messages[1]. Augustus Ceaser used shifting by four places. By the time the computers came into existence and breaking 'shifting by three or four places code' was just a pen and paper work, so the need of more competent techniques grown. Then the generation of encryption by ASCII keys and other methods came into existence. As the time passed the encrypted data was not sent by directly. But it was still modified by some algorithms such as RSA, Rabin, Algamal, McEliece, Knapsack and Probabilistic public key transferring algorithms[2]. All of these algorithms in the present literature are based on large prime numbers or on a part of number theory. None of the pioneers have concentrated on the functional analysis or metric spaces. We introduce an algorithm which is based on the concepts of contractive functions in Banach spaces, Banach contraction principle, fixed points and unique prime factorisation of a positive integer.

Here, we introduce a new technique of encryption which is based on Banach Contraction Principle of fixed point theory and Unique Factorisation theorem of number theory.

2. Preliminaries

2.1. Definition [3]

Let V be a linear/ vector space over the field $\mathbb{F}(=\mathbb{C}\ or\ \mathbb{R})$. A norm on V is a mapping/ function $\|\cdot\|$ from V to $\mathbb{R}_0^+$,

$$\|.\|: V \to \mathbb{R}_0^+,$$

Satisfying the following three axioms:

(N1) $\|u\| = 0 \Longrightarrow u = 0$ [positivity]

(N2) $\|\lambda u\| = |\lambda|\|u\|$ for all $u \in V$ and all $\lambda \in \mathbb{F}$ [homogeneity]

(N3) $\|u + v\| \leq \|u\| + \|v\|$ for all $u, v \in V$ [triangle inequality]

We call the pair $(V, \|\cdot\|)$, a normed space.

2.2. Convergence to a Limit [3]

Let $\|\cdot\|$ be a norm on a vector space V over $\mathbb{F}$. We say that a sequence $\{u_n\}$ of vectors in V converges to a vector $u \in V$ with respect to the norm $\|\cdot\|$, written as, $\lim_{n\to\infty} u_n = u$, if for each $\epsilon > 0$, there exists a natural number $N = N(\epsilon)$, such that, $\|u_n - u\| < \epsilon$ whenever $n \geq N$.

2.3. Cauchy Sequence [3]

The sequence $\{u_n\}$ in a normed space $(V, \|\cdot\|)$ is called a Cauchy sequence if for every $\epsilon > 0$, there exists a positive integer $N = N(\epsilon)$, such that, $\|u_m - u_n\| < \epsilon$ whenever $m, n \geq N$.

2.4. Complete Normed Linear Space[3]

$(V, \|\cdot\|)$ is called a complete normed space if for every sequence $\{u_n\}$ in V, such that, $\|u_n - u_m\| \to 0$ as $n, m \to \infty$ there exists an element $u \in V$, such that, $\|u_n - u\| \to 0$ as $n \to \infty$.

2.5. Definition (Banach Space) [3]

A Banach space is a complete normed linear space.

2.6. Theorem [3]

In a Banach space, a sequence is convergent if and only if it is Cauchy.

2.7. Theorem (Banach Fixed Point Theorem) [4]

Let K be a complete metric space in which the distance between two points P and Q is denoted $d(P,Q)$. And let $F: K \to K$ be a contraction, i.e., there exists $c \in (0,1)$ such that for all $P, Q \in K$,

$$d\left(F\left(P\right),F\left(Q\right)\right) \leq cd\left(P,Q\right).$$

Then, F has a unique fixed point, i.e., there exists a unique $A \in K$ such that $F(A) = A$.

3. The Proposed Scheme for Encryption

Each of the alphabet, integer or the special character is hereby associated with a contractive function whose fixed point is a prime number. One of such scheme is given as follows:

$$A = 1 + \frac{x}{2},$$
$$with\ fixed\ point\ x = 2$$
$$B = 1 + \frac{2x}{3},$$
$$with\ fixed\ point\ x = 3$$
$$C = 1 + \frac{4x}{5},$$
$$with\ fixed\ point\ x = 5$$
$$D = 1 + \frac{6x}{7},$$
$$with\ fixed\ point\ x = 7$$
$$E = 1 + \frac{10x}{11},$$
$$with\ fixed\ point\ x = 11$$
$$F = 1 + \frac{12x}{13},$$
$$with\ fixed\ point\ x = 13$$
$$G = 1 + \frac{16x}{17},$$
$$with\ fixed\ point\ x = 17$$
$$H = 1 + \frac{18x}{19},$$
$$with\ fixed\ point\ x = 19$$
$$I = 1 + \frac{22x}{23},$$
$$with\ fixed\ point\ x = 23$$
$$J = 1 + \frac{28x}{29},$$
$$with\ fixed\ point\ x = 29$$
$$K = 1 + \frac{30x}{31},$$
$$with\ fixed\ point\ x = 31$$
$$L = 1 + \frac{36x}{37},$$
$$with\ fixed\ point\ x = 37$$
$$M = 1 + \frac{38x}{39},$$
$$with\ fixed\ point\ x = 39$$
$$N = 1 + \frac{40x}{41},$$
$$with\ fixed\ point\ x = 41$$
$$O = 1 + \frac{42x}{43},$$
$$with\ fixed\ point\ x = 43$$
$$P = 1 + \frac{46x}{47},$$
$$with\ fixed\ point\ x = 47$$
$$Q = 1 + \frac{52x}{53},$$
$$with\ fixed\ point\ x = 53$$
$$R = 1 + \frac{58x}{59},$$
$$with\ fixed\ point\ x = 59$$
$$S = 1 + \frac{60x}{61},$$
$$with\ fixed\ point\ x = 61$$
$$T = 1 + \frac{66x}{67},$$
$$with\ fixed\ point\ x = 67$$
$$U = 1 + \frac{70x}{71},$$
$$with\ fixed\ point\ x = 71$$
$$V = 1 + \frac{72x}{73},$$
$$with\ fixed\ point\ x = 73$$
$$W = 1 + \frac{78x}{79},$$
$$with\ fixed\ point\ x = 79$$
$$X = 1 + \frac{82x}{83},$$
$$with\ fixed\ point\ x = 83$$
$$Y = 1 + \frac{88x}{89},$$
$$with\ fixed\ point\ x = 89$$
$$Z = 1 + \frac{96x}{97},$$
$$with\ fixed\ point\ x = 97$$

$$a = 1 + \frac{100x}{101}, \text{ with fixed point } x = 101$$

$$b = 1 + \frac{102x}{103}, \text{ with fixed point } x = 103$$

$$c = 1 + \frac{106x}{107}, \text{ with fixed point } x = 107$$

$$d = 1 + \frac{108x}{109}, \text{ with fixed point } x = 109$$

$$e = 1 + \frac{112x}{113}, \text{ with fixed point } x = 113$$

$$f = 1 + \frac{126x}{127}, \text{ with fixed point } x = 127$$

$$g = 1 + \frac{130x}{131}, \text{ with fixed point } x = 131$$

$$h = 1 + \frac{136x}{137}, \text{ with fixed point } x = 137$$

$$i = 1 + \frac{138x}{139}, \text{ with fixed point } x = 139$$

$$j = 1 + \frac{148x}{149}, \text{ with fixed point } x = 149$$

$$k = 1 + \frac{150x}{151}, \text{ with fixed point } x = 151$$

$$l = 1 + \frac{156x}{157}, \text{ with fixed point } x = 157$$

$$m = 1 + \frac{162x}{163}, \text{ with fixed point } x = 163$$

$$n = 1 + \frac{166x}{167}, \text{ with fixed point } x = 167$$

$$o = 1 + \frac{172x}{173}, \text{ with fixed point } x = 173$$

$$p = 1 + \frac{178x}{179}, \text{ with fixed point } x = 179$$

$$q = 1 + \frac{180x}{181}, \text{ with fixed point } x = 181$$

$$r = 1 + \frac{190x}{191}, \text{ with fixed point } x = 191$$

$$s = 1 + \frac{192x}{193}, \text{ with fixed point } x = 193$$

$$t = 1 + \frac{196x}{197}, \text{ with fixed point } x = 197$$

$$u = 1 + \frac{198x}{199}, \text{ with fixed point } x = 199$$

$$v = 1 + \frac{210x}{211}, \text{ with fixed point } x = 211$$

$$w = 1 + \frac{222x}{223}, \text{ with fixed point } x = 223$$

$$x = 1 + \frac{226x}{227}, \text{ with fixed point } x = 227$$

$$y = 1 + \frac{228x}{229}, \text{ with fixed point } x = 229$$

$$z = 1 + \frac{232x}{233}, \text{ with fixed point } x = 233$$

$$\text{white space} = 1 + \frac{238x}{239}, \text{with fixed point } x = 239$$

$$! = 1 + \frac{240x}{241}, \text{ with fixed point } x = 241$$

$$@ = 1 + \frac{250x}{251}, \text{ with fixed point } x = 251$$

$$\# = 1 + \frac{256x}{257}, \text{ with fixed point } x = 257$$

$$\$ = 1 + \frac{262x}{263}, \text{ with fixed point } x = 263$$

$$\% = 1 + \frac{268x}{269}, \text{ with fixed point } x = 269$$

$$\wedge = 1 + \frac{270x}{271}, \text{ with fixed point } x = 271$$

$$\& = 1 + \frac{276x}{277},$$

$$with\ fixed\ point\ x = 277$$
$$*= 1 + \frac{280x}{281},$$
$$with\ fixed\ point\ x = 281$$
$$(= 1 + \frac{282x}{283},$$
$$with\ fixed\ point\ x = 283$$
$$) = 1 + \frac{292x}{293},$$
$$with\ fixed\ point\ x = 293$$
$$\cong 1 + \frac{306x}{307},$$
$$with\ fixed\ point\ x = 307$$
$$` = 1 + \frac{310x}{311},$$
$$with\ fixed\ point\ x = 311$$
$$" = 1 + \frac{312x}{313},$$
$$with\ fixed\ point\ x = 313$$
$$' = 1 + \frac{316x}{317},$$
$$with\ fixed\ point\ x = 317$$
$$[= 1 + \frac{330x}{331},$$
$$with\ fixed\ point\ x = 331$$
$$] = 1 + \frac{336x}{337},$$
$$with\ fixed\ point\ x = 337$$
$$\{= 1 + \frac{346x}{347},$$
$$with\ fixed\ point\ x = 347$$
$$\} = 1 + \frac{348x}{349},$$
$$with\ fixed\ point\ x = 349$$
$$\backslash= 1 + \frac{352x}{353},$$
$$with\ fixed\ point\ x = 353$$
$$/= 1 + \frac{358x}{359},$$
$$with\ fixed\ point\ x = 359$$
$$.= 1 + \frac{366x}{367},$$
$$with\ fixed\ point\ x = 367$$
$$?= 1 + \frac{372x}{373},$$
$$with\ fixed\ point\ x = 373$$
$$,= 1 + \frac{378x}{379},$$
$$with\ fixed\ point\ x = 379$$
$$<= 1 + \frac{382x}{383},$$
$$with\ fixed\ point\ x = 383$$
$$>= 1 + \frac{388x}{389},$$
$$with\ fixed\ point\ x = 389$$
$$;= 1 + \frac{396x}{397},$$
$$with\ fixed\ point\ x = 397$$
$$:= 1 + \frac{400x}{401},$$
$$with\ fixed\ point\ x = 401$$
$$-= 1 + \frac{408x}{409},$$
$$with\ fixed\ point\ x = 409$$
$$\_ = 1 + \frac{418x}{419},$$
$$with\ fixed\ point\ x = 419$$
$$+= 1 + \frac{420x}{421},$$
$$with\ fixed\ point\ x = 421$$
$$== 1 + \frac{430x}{431},$$
$$with\ fixed\ point\ x = 431$$
$$| = 1 + \frac{432x}{433},$$
$$with\ fixed\ point\ x = 433$$

Now, after defining the codes of our encryption, we propose the algorithm for coding. The message will be encoded as two different numbers one which we get by getting the fixed point of the composition and one is the multiplication of the respective prime numbers.

4. Algorithms

4.1. Algorithm for the Encryption

1) Consider the characters used in the message as the functions as defined and the functions are connected as the compositions. i.e., "gauss" will be treated as "$g\left(a\left(u\left(s(s(x))\right)\right)\right)$".
2) Find out the fixed point of the function derived from step 1.
3) Now, again consider the characters in the message as corresponding prime numbers. i.e., "g=131, a=101, and so on".
4) Multiply these primes to get a unique composite number.
5) The fixed point of step 2 and the composite number in step 4 are the required encryptions.

4.2. Algorithm for the Decryption

1) Factorize the composite number to get a unique prime factorisation.

2) Write down the corresponding characters to the prime numbers.
3) Now, to get the correct sequence of the characters locate the composite function having the fixed point encrypted.
4) The sequence of characters so derived is the required message.

4.3. Example

Let, the message to be sent is "one". Then, first we find the composition function

$$o\left(n\left(e\left(x\right)\right)\right)=1+\frac{172}{173}\left(1+\frac{162}{163}\left(1+\frac{112x}{113}\right)\right)$$

with the fixed point $x=\frac{9503187}{65719}$.

Again, the composite number is $o=173, n=163, e=113 \Rightarrow 173\times 163\times 113=3186487$. Now, our required encryption is: $\frac{9503187}{65719}$ and 3186487.

Now, to decrypt the message again we first factorize the composite number, i.e., $3186487=113\times 163\times 173$. Now, $113=e, 163=n, 173=o$. But this can imply six combinations: viz, eno, eon, neo, noe, oen, one.

Now,

$$e\left(n\left(o\left(x\right)\right)\right)$$
$$=1+\frac{112}{113}\left(1+\frac{162}{163}\left(1+\frac{172x}{173}\right)\right)$$
$$=\frac{9483687}{65719},$$
$$e\left(o\left(n\left(x\right)\right)\right)$$
$$=1+\frac{112}{113}\left(1+\frac{172}{173}\left(1+\frac{162x}{163}\right)\right)$$
$$=\frac{9484807}{65719},$$
$$n\left(e\left(o\left(x\right)\right)\right)$$
$$=1+\frac{162}{163}\left(1+\frac{112}{113}\left(1+\frac{172x}{173}\right)\right)$$
$$=\frac{9492337}{65719},$$
$$n\left(o\left(e\left(x\right)\right)\right)$$
$$=1+\frac{162}{163}\left(1+\frac{172}{173}\left(1+\frac{112x}{113}\right)\right)$$
$$=\frac{9502057}{65719},$$
$$o\left(e\left(n\left(x\right)\right)\right)$$
$$=1+\frac{172}{173}\left(1+\frac{112}{113}\left(1+\frac{162x}{163}\right)\right)$$
$$=\frac{9466551}{65719},$$
$$o\left(n\left(e\left(x\right)\right)\right)$$
$$=1+\frac{172}{173}\left(1+\frac{162}{163}\left(1+\frac{112x}{113}\right)\right)$$
$$=\frac{9503187}{65719}.$$

So, the one combination that has the same fixed point as per our encryption is "one". And hence the given encryption is accurate as per the given conditions.

4.4. Example

Let, the message to be sent is "Gauss!". Then, the composition function is

$$G\left(a\left(u\left(s\left(s\left(!\left(x\right)\right)\right)\right)\right)\right)$$
$$=1+\frac{16}{17}\left(1+\frac{100}{101}\left(1+\frac{198}{199}\left(1+\frac{192}{193}\left(1+\frac{192}{193}\left(1+\frac{240x}{241}\right)\right)\right)\right)\right)$$

with the fixed point $x=\frac{17300053241203}{264447718147}$.

Again, the composite number is $17\times 101\times 199\times 193\times 193\times 241=3067291366147$. Now, our required encryption is: $\frac{17300053241203}{264447718147}$ and 3067291366147.

Now, to decrypt the message again we first factorize the composite number, i.e., $3067291366147=17\times 101\times 199\times 193\times 193\times 241$. Now, $17=G, 101=a, 199=u, 193=s, 241=!$. But, keeping G at first place and ! at the last place, we still have $\frac{4!}{2!}$ ways to arrange the message: Gauss!, Gasus!, Gassu!, Guass!, Gusas!, Gussa!, Gsaus!, Gsasu!, Gsuas!, Gsusa!, Gssua!, Gssau!

$$Gauss!=\frac{17300053241203}{264447718147}$$
$$Gasus!=\frac{17299606718403}{264447718147}$$
$$Gassu!=\frac{17299162505203}{264447718147}$$
$$Guass!=\frac{17314129191315}{264447718147}$$
$$Gusas!=\frac{17327685684243}{264447718147}$$
$$Gussa!=\frac{17341171936275}{264447718147}$$
$$Gsuas!=\frac{17327234694195}{264447718147}$$
$$Gsusa!=\frac{17340720946227}{264447718147}$$
$$Gsasu!=\frac{17312787465267}{264447718147}$$
$$Gssua!=\frac{17340272292915}{264447718147}$$
$$Gssau!=\frac{17326341829683}{264447718147}$$

So, the one combination that has the same fixed point as per our encryption is “Gauss!”.

5. Advantages

The given algorithm is different from the routine encryptions. The routine encryptions decode the data as large integers. These encryptions cannot be sent as it is, since the data can be decrypted easily using different algorithm. For example one can first identify the most frequently occurring code and assume that to be the letter “a”, as “a” is the most frequently occurring alphabet. And then accordingly find out the white space and other tentative guesses. Hence, the codes can sometimes be even broken by pure guessing.

Now, even if by factorising the code one can guess that the prime with highest power is “a”, still the person does not know, where to place these “a”. Again, one can only guess that this letter is “a”, but the corresponding function cannot be known as there are many functions whose fixed point can be the given prime number.

In order to secure this routinely encrypted data one has to use one or the other public key algorithms, but the algorithm presented in this paper is self dependent to secure the data. However, the public key algorithms can be used to secure the data even to a higher degree.

6. Conclusion

The algorithm presented in the article is a new approach of encoding the secret messages, which contrary to the schemes present in the literature uses contractive functions and the concept of fixed point theorems. The algorithm is technically sound and is thoroughly verified for accuracy. This concept provides a new vision to the cryptography which till date relies only on the number theory for the security.

7. Scope of the Study

The paper discusses the algorithm in a banach space of real numbers. The same algorithm can be discussed in different spaces using appropriate properties of functions. The concept of prime numbers is used in the algorithm for which one has to take the whole set of real numbers. So if we find a substitution of prime numbers in the functions itself then on can even take the bounded spaces, like [0,1].

References

[1] W. Trappe, L.C. Washington, “Introduction to Cryptography with Coding Theory”, Pearson Education International, Prentice Hall (Second Edition).

[2] A. J. Menezes, P. C. van Oorschot, S. A. Vanstone “Handbook of Applied Cryptography”, CRC Press, 1996, 816 pages.

[3] S. Punnusamy, “Foundations of Functional Analysis”, CRC Press, 2002, 457 pages.

[4] Christiane Rousseau “Banach Fixed Point Theorem and Applications”, Universite de Montreal, 2010.