Elliptic Curves, Palindrome Numbers and Secret keys

Karuna Kamath K.
NMAM Institute of Technology,
NItte- 574 110, India

Shankar B.R
National Institute of Technology Karnataka,
Surathkal- 575 025,

ABSTRACT

A secret key generation scheme based on points on Elliptic curves and palindromes is presented in this paper. These keys could be used as One Time Pads for secure transaction. Our method generates keys of variable size randomly. The procedure can be easily deployed in security –sensitive systems to reduce the damage caused by hacking the data.

Keywords

Palindromes, Elliptic curve, Fibonacci sequence, Stream cipher, Random number.

1. INTRODUCTION

1.1 Elliptic curves

For any prime p, let Fp denote the field of integers modulo p. An elliptic curve, E, over Fp is an equation of the form $y^2 = x^3 + ax^2 + b x + c$, where a, b, c ε Fp with $4a^3 + 27b^2 \neq 0$(mod p). Using suitable transformation of the coordinates this can be put in the form$y^2 = x^3+ax+b$, called the standard form. The set of all points on E denoted by E (Fp) forms an abelian group with ∞, the point at infinity serving as the identity element with respect to addition [1][2]. The addition operation is defined as below:

Let $P_1(x_1, y_1)$ and $P_2(x_2, y_2)$ be 2 points such that

$P_{1,} P_2 \neq\infty$

1. If $x_1 \neq x_2$, $x_3 = m - x_1 - x_2,$ $y_3 = m(x_1 - x_3) - y_1$, where $m = (y_2 - y_1) / (x_2 - x_1)$.

2. If $x_1 = x_2$ but $y_1 \neq y_2$, $P_1 + P_2 = \infty$

3. If $P_1 = P_2$ and $y_1 \neq 0$; $x_3 = m^2 - 2x_1$ and

$y_3 = m(x_1 - x_3) - y_1$, where $m = (3x^2_1 + a) /2y_1$.

4. If $P_1 = P_2$ and $y_1 = 0$ then $P_1 + P_2 = \infty$

1.2 Palindromes via reverse and add

Beginning with the decimal representation of any integer N, reverse the digits and add it to N. Repeat this operation to arrive at a palindrome[3][4].

For example, starting with 79 we get, after six iterations, a palindrome:

79 + 97 = 176

176 + 671 = 847

847 + 748 = 1595

1595 + 5951 = 7546

7546 + 6457 = 14003

14003 + 30041 = 44044

1.3 Steganography

Due to the advancement in technologies most people use the internet as the medium to transfer data to and fro across the world. The data transmission is very simple and fast using the internet. But one of the main disadvantages with sending data over the internet is the security of the personal or confidential data. So data security is the most important factor that needs to be considered during the transmission of data. Data security means protection of data from unauthorized users. Data security is gaining more attention due to the enormous use of the internet for data transmission. Data security can be provided using different techniques like: Cryptography and Steganography. Cryptography is a method to mask the information by encrypting and transmitting using a secret key. Steganography provides security by hiding the encrypted message into an apparently invisible image or other formats. Steganography is the science of hiding information [12]. Steganography involves hiding data in an overt message and doing it in such a way that it is difficult for an adversary to detect and remove [5][7]. Digital steganography is usually based on the least significant bit [6][8]. Since the least significant bit has little effect on the actual color, human viewers are unlikely to notice. Bitmaps, jpegs and other formats can all easily carry hidden messages in the least significant bit of the color. Image steganography is the science of hiding data inside cover images for security [9][10]. Images have a lot of visual redundancy in the sense that our eyes do not usually care about subtle changes in color in an image region. One can use this redundancy to hide text, audio or even image data inside cover images without making significant changes to the visual perception.

Steganographic process can be described as follows:

cover_image + message + secret key = stego_image

The cover_image is the file in which we hide the data, which may also be encrypted using the secret key. The resultant file is the stego_image.

2. ELLIPTIC CURVES AND SECRET KEYS

Select an Elliptic Curve E over a finite field Fp. We choose two points on the curve E and apply the (2, 1) Lagged Fibonacci generator to get a sequence of points on the curve E which is fairly random [11] Pick any one point(x, y) ε E and apply the "Reverse and Add" procedure to the X-coordinate 'x' until a palindrome is obtained. All the numbers got in this procedure are concatenated to obtain a fairly random string at the end. This string can be used as the secret key.

The Algorithm:

a) Key = " ".
b) Choose two points (x_1, y_1) and(x_2, y_2) on the selected elliptic curve and apply the (2, 1) Lagged Fibonacci generator to get a sequence of points on the curve E.
c) Select any point (x, y) from the sequence and take x as the seed.
d) Test for palindrome. If yes go to step (g).
e) Reverse the sum and add to the sum to get new sum.
f) Concatenate this sum to the Key. Go to step (d).
g) Concatenate this to the Key.

x = 79 Rev = 97; Sum = 176; Key =176

Rev= 671; Sum =176 + 671 = 847;

Rev= 7488; Sum = 847 + 748 = 1595;

Rev= 5915; Sum = 1595 + 5951 = 7546;

Rev = 6457; Sum= 7546 + 6457 = 14003;

Rev = 30041;

Sum = 14003 + 30041 = 44044;

Key =17684715957546140034404 is the

secret key.

x = 132; Rev =231; Sum = 363; Key 363 is

the secret key.

3. EXPERIMENTAL RESULTS

E : $y^2 = x^3 + x + 1$; p= 1023.

Table 3.1 points on E and corresponding Keys

Sl. No	Point on E	Key
1	(79,132)	17684715957546140034404
2	(190,400)	28146382715557106131234525 4
3	(693,374)	10891089020691402937949 7
4	(286,684)	096818379218173479171817343790780817165178872688177354768518924715948740566427235613175448223602001953719300401613297007933472670871649344516343817688131787795559450654818012000021078813200023188
5	(276,116)	094817979768184479292817585793442817588679447438177948879664465818228932790627160817124442178836886388

Analysis of keys in terms of occurrences of the digits 0, 1 2, - -- -- -, 9.

Table 3.2 frequency of digits in the keys
Chi-Square test results at 1%, 5% and 10% levels of significance

Table 3.3 Chi-Square test results

Sl. No	Test value	Accepted/Rejected		
		1%	5%	10%
1	14.31	A	A	A
2	8.91	A	A	A
3	12.6	A	A	A
4	16.74	R	A	A
5	27.99	R	R	R

4. APPLICATION

The keys generated are used in digital Steganography. The procedure is represented by the Fig 4.1 Message is embedded in the cover image using the key at the source end and using the same key the message is recovered at the receiver end.

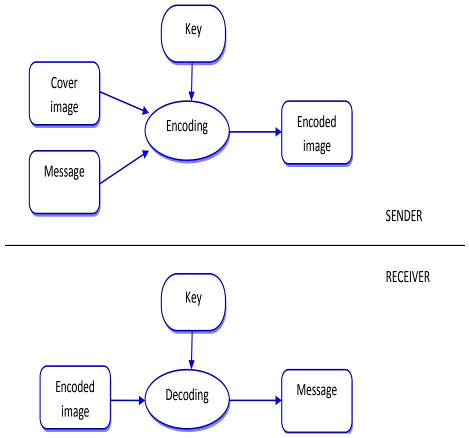


Fig 4.1 Digital Steganography Block Diagram

Fig 4.2 a) and 4.2 c) shows the bmp files before and after embedding message using the key. We observe no noticeable differences in these bmp files. The enhanced LSB representation of the cover_image Fig 4.3 a) and Stego_image Fig 4.3b). Enhanced LSB's also properly concealed the content. The histograms of the original and embedded images are given by Fig 4.4 a) and Fig4.4 b). There are no perceptible differences between the histograms of original and Stego_image. Another way of detecting steganography is statistical analysis [12]. The output of a chi-square analysis on the cover_image 4.5 a) and Stego-image 4.5 b) are quite similar.

Sl. No	Digits									
	0	1	2	3	4	5	6	7	8	9
1	3	3	0	1	7	3	2	3	1	1
2	1	5	4	3	3	5	2	2	2	0
3	5	3	2	1	2	0	1	2	2	6
4	23	28	14	19	17	14	14	28	25	13
5	3	10	9	5	14	4	9	16	21	11

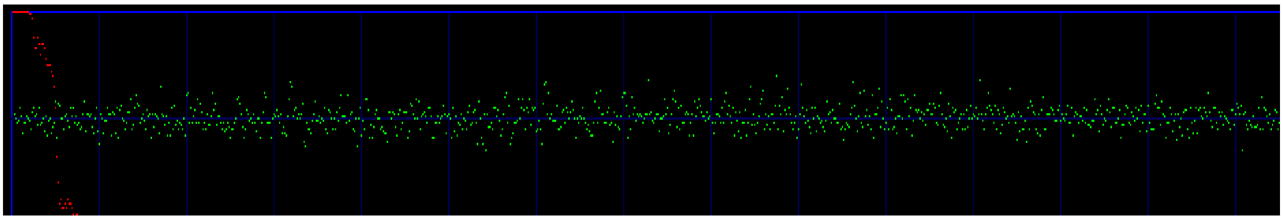


Fig 4.5 a) Output of a chi-square analysis on the cover_image

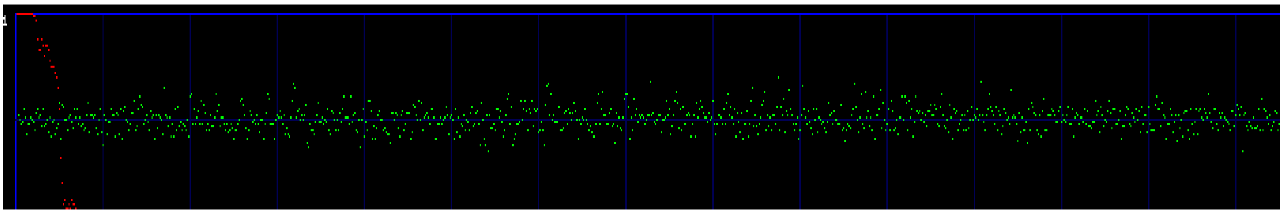
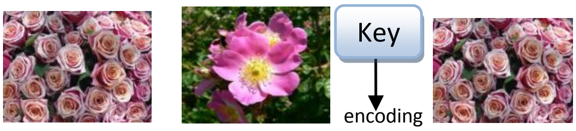


Fig 4.5 b) Output of a chi-square analysis on the Stego-image



4.2 a) Cover-image 4.2b) message image 4.2 c)

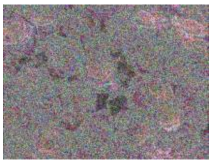


Fig 4.3 a) LSB cover_image

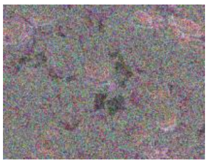


Fig 4.3 b) LSB Steg_image

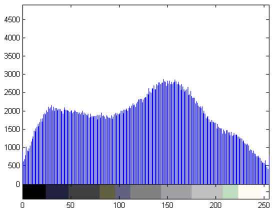


Fig 4.4 a) Histogram Cover_image

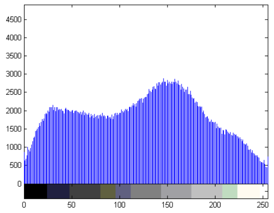


Fig 4.4 b) Histogram Stego_image

5. CONCLUSION

The secret key generation scheme proposed in this paper is fast and keys of varied size are generated. The important point to note is that the key length varies with the starting number and more significantly, depends on the number of iterations required to generate the palindrome number. The randomness of the keys suggests the usage for encryption applications.

6. REFERENCE

[1] Neal Koblitz, " A Course in Number Theory and Cryptography" Springer- verlag , Second Edition ,1994.

[2] William Stallings, "Cryptography and Network Security: Principles and Practices", PHI, 2005, Fourth Edition.

[3] 196 Palindrome Quest, Most Delayed Palindromic Number: http://www.jasondoucette.com/worldrecords.html

[4] John Walker, "Three Years of Computing Final Report on the Palindrome Quest", http://www.fourmilab.ch/documents/threeyears/threeyears.html

[5] Steganography and Steganalysis J.R. Krenn January 2004 http://www.krenn.nl/univ/cry/steg/article.pdf

[6] http://iwearshorts.com/Mike/uploads/2011/06/10.1.1.62.8194.pdf

[7] Hide and Seek: An Introduction to Steganography, NIELS PROVOS AND PETER HONEYMAN University of Michigan.

[8] Improved Detection of LSB Steganography in Grayscale Images by Andrew D. Ker

http://www.cs.ox.ac.uk/andrew.ker/docs/ADK09D.pdf

[9] T Morkel, JHP Eloff and MS Olivier, "An Overview of Image Steganography," *in* Proceedings of the Fifth Annual Information Security South Africa Conference

(ISSA2005), Sandton, South Africa, June/July 2005.

[10] Reliable Detection of LSB Steganography in Color and Grayscale Images by Jessica Fridrich

http://faculty.ksu.edu.sa/ghazy/Steg/References/ref26-2.pdf

[11] Shankar B R, Karuna Kamath K, “(2,1) Lagged Fibonacci Generators Using Elliptic Curves over Finite Fields”, Proceedings of International Conference on Computer Engineering and Technology, Vol 2, pp 456-457, 22-24 Jan 2009, Singapore.

[12] Cole, E., Hiding in Plain Sight: “Steganography and the Art of Covert Communication”, Canada: 2003 Wiliey Publishing.