American International Journal of Business Management (AIJBM)
ISSN- 2379-106X, www.aijbm.com Volume 04, Issue 05(May-2021), PP 20-23

BRA Symmetric Encryption Algorithm

Remzi AKTAY[1]
[1]Keçiören ŞehitHalilIşılar Middle School/ Ankara/TURKEY

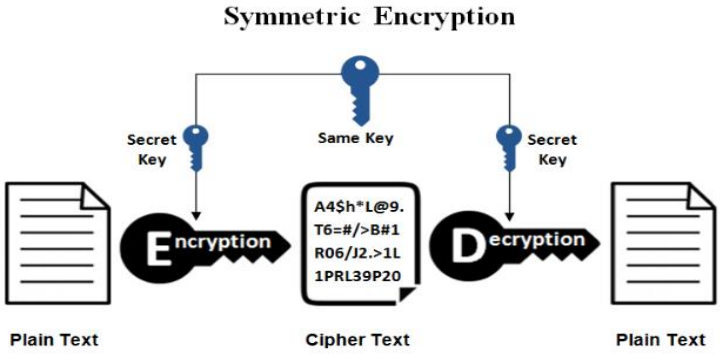
Abstract: In this study, it is tried to develop a symmetric encryption algorithm. As it is known, the sender and receiver keys are the same in symmetric encryption algorithms. Based on the rule of finding the third point based on the two points taken on elliptic curves, it has been investigated whether this rule can be used in lines that intersect both axes. It has been found that the desired rule is also satisfied in the correct equations. In addition, when the rule of finding the third point is applied on lines that intersect both axes, it has been discovered that the same points come once again at three points. Symmetric encryption was possible with the help of this feature. In the encryption algorithm, the ASCII character code of each character to be encrypted is written as the sum of 10 numbers. Random keys consisting of 10 numbers were generated against these 10 numbers. In the key consisting of 10 numbers and 10 numbers representing the ASCII Character Code, the corresponding numbers will not be the same. In this way, the slope is prevented from becoming undefined or zero. The important thing here is that the key and ASCII Character Code must be written as the sum of even numbers, since the rule to find the third point from two points will be applied. For simplicity in our algorithm, the character's ASCII Character Code is written as the sum of 10 numbers. When the software is made, it can be written as the sum of infinite numbers if desired, and in turn, infinite different keys can be created. In this respect, it differs from other symmetric encryption algorithms. In this algorithm, there are 5 different line equations, since the rule of finding the third point will be applied from the beginning to the binary numbers among the 10 numbers representing the 10 numbers in the key and the 10 numbers representing the character code. The deciphering process will be very complex, since a third person who finds the encrypted numbers cannot know neither the lines nor the slopes. When the software is made, it can be used in all areas where symmetric encryption algorithms are used.

Keywords: Slope, Equations of the line, key, Encryption, Algorithm,

I. Introduction

In this study, it is aimed to develop a symmetric encryption algorithm.
Elliptic Curves, with the general equation a, b being a real number;
$y^2 = x^3 + a.x + b$. As seen in Figure-1, the coordinates of the P (x_3, y_3) point for the m_1 (x_1, y_1) and m_2 (x_2, y_2) points taken over the elliptic curves are as follows; Let s be the slope of the line passing through the points m_1 and m_2. The coordinates of the point P (x_3, y_3) such that $x_3 = s^2-x_1-x_2$ and $y_3 = s.(x_1-x_3) - y_1$. The point m_3 $(x_3, -y_3)$, which is the symmetry of the point P with respect to the x-axis, is again a point on the elliptic curve (Yücelen, M. 2017)

Then, computer coding types were investigated. BCD (Binary Coded Decimal), Oktal BCO Binary, Hegzadecimal BCH Binary, Decimal BCD, 3 redundant and Gray encodings are some of them (Kodaz, H. 2010).



(Figure -1)

As seen in Figure-1, the same key is used in symmetric encryption algorithms. Some of the algorithms developed so far are DES, AES, Blowfish, Twofish, IRON. DES, developed by IBM, is one of the most used symmetric encryption algorithms in the world. Using block encryption, DES encrypts 64-bit data using a 56-bit key during the transaction. The key was broken in the early 2000s due to its short length. On top of that, it was developed as Triple-DES, that is, 3DES. 3DES is the use of DES 3 times in a row. In other words, it is 3 times

slower than normal DES, but it is used in applications such as SSH today. DES lost its popularity upon the release of AES. It is already 6 times slower than AES. After the DES was broken, a new search was started and AES symmetric encryption algorithm was created in 2001. DES's weaknesses are hardened and it uses the block cipher algorithm. It is 6 times faster than AES. It supports 128, 192 and 256 bit keys in length. It is one of the most popular algorithms today and is thought to be resistant to brute force attacks. The Blowfish algorithm, which was suddenly popular for its free, is one of the fastest cryptographers on the market, making it difficult to crack using complex key tables. Blowfish has key lengths from 23 to 448 bits. It needs at least 4 kb of RAM to run, which makes it unusable in embedded systems. Twofish algorithm, which is as fast as AES, uses Feistal structure like DES, but unlike DES, it has S-boxes through the key. It processes texts by splitting them into 32-bit pieces and works as a block algorithm. Different encryption and decryption algorithms slowed down applications by 5% and increased the cost. Using the Feistel structure, IRON encrypts 64-bit data blocks with a 128-bit key and operates with 16 to 32 cycles. The advantage of this algorithm is that it is used for base 16 numbers rather than bits, the disadvantage is that it is designed for software (Levi, A. &Özcan, M. 2010)

II. Method

2.1. Compliance of the Rule of Elliptic Curves in Line Equations that Cross Two Axes

Elliptic Curves, the general equation a, b being a real number; $y^2= x^3 + a.x + b$. The coordinates of the point P (x_3, y_3) for the m_1 (x_1, y_1) and m_2 (x_2, y_2) points taken over the elliptic curves are as follows;

Let s be the slope of the line passing through the points m_1 and m_2.

The coordinates of the point P (x_3, y_3) such that $x_3 = s^2-x_2-x_1$ and $y_3 = s. (x_1-x_3) –y_1$.

The point m_3 $(x_3, -y_3)$, which is the symmetry of the point P with respect to the x axis, is again on the elliptic curve. Let's prove whether this method satisfies in the correct equation.

Let $y = s.x + b$ be our line equation. ……(1)

If m_2 (x_2, y_2) is on the line, it must provide the right.

$y = s. x_2 + b$, then $b = y_2 - s. x_2$. ……..(2)

$x_3 = s^2-x_2-x_1$

$y_3 = s. (x_1-x_3) –y_1$ ……. (3)

When y_3 is written instead of x_3;

$y_3 = s. (x_1-s^2 + x_2 + x_1) –y_1 = 2.s.x_1- s^3 + s.x_2 –y_1$. ……(4)

Suppose that for point P (x_3, y_3), point P ”$(x_3, -y_3)$ satisfies the line equation. In this case, let's write this point in place of (1).

$- (2.s.x_1- s^3 + s.x_2) + y_1 = s. (s^2-x_2-x_1) + b$ ……(5)

When (2) is written instead of (5);

$-2.s.x_1 + s^3-s.x_2 = s. (s^2-x_2-x_1) + y_2 - s. x_2$ ……. (6)

$-2.s.x_1 + s^3-s.x_2 + y_1 = s^3-s.x_2-s.x_1 + y_2 - s. x_2$

$-2.s.x_1-s.x_2 + y_1 = -2.s.x_2-s.x_1 + y_2$

If $s.x_2-s.x_1 = y_2-y_1$ then $s. (x_2-x_1) = y_2-y_1$

The equation $s = (y_2-y_1) / (x_2-x_1)$ comes out.

2.2. Properties of the Rule of Finding the Third Point in Lines Crossing Axes

The rule used in elliptic curves is valid for lines intersecting axes as shown in 3.1.

Let the third point be C $(x_3, -y_3)$ from point A (x1, y1) with respect to point B (x_2, y_2). Now let's find the third point with respect to the point C $(s^2-x_1-x_2, -s. (x_1-x_3) + y_1)$ from the point B (x_2, y_2) in order. Let this point be D (x_4, y_4). Since the points B and C are on the same line, the slope is the same and it is "s".

$x_4 = s^2- x_2 - (s^2-x_1-x_2) = x_1$.

$y_4 = -s. (x_2- x_1) + y_2 = - (y_2-y_1) / (x_2-x_1)$. Definition of slope $(x_2 – x_1) + y_2$ $s = (y_2-y_1) / (x_2-x_1)$

take $y_4 = y_1$. As you can see, the third point is the point A (x_1, y_1). In this way, when the third point finding rule is applied sequentially;

It continues as A –B - C - A - B - C- …… ... When we examined elliptic curves, we could not find such a feature.

III. Results

The following findings were reached in this study.

3.1. Finding the Third Point from Two Points on the Line

The rule of finding the third point used in Elliptic Curves is also provided in line equations. In our investigations, when we apply the rule of finding the third point for two consecutive points, unlike elliptic curves, the line wraps around three points.

Example 1: Let's apply the rule to find the 3rd point for the line passing through the points A (0,6) and B (-3,0), respectively.

$s = (6-0) / (0 - (- 3)) = 2$.

$m_1 (x_1, y_1) = m1 (0, 6)$. $m_2 (x_2, y_2) = m_2 (-3, 0)$.
$x_3 = 2^2 -0 - (- 3) = 7$.
$y_3 = 2. (0-7) -6 = -20$ P (7, -20) Point C (7,20), which is symmetrical with respect to the x-axis, is again on the line.
Now let's find the 3rd point with respect to the point B (-3,0) and C (7,20).
s = 2, $m_1 (x_1, y_1) = m_1 (-3, 0)$ $m_2 (x_2, y_2) = m_2 (7, 20)$.
$x_3 = 22 - (- 3) -7 = 0$.
$Y_3 = 2. (- 3-0) -0 = -6$.P is (0, -6). The point that is symmetrical with respect to the x-axis becomes point A (0,6). Applying the third point finding rule to point C and A respectively, point B comes out.

3.2. Writing ASCII Character Codes in 10 Numbers

The codes of ASCII Characters will be written as the sum of 10 numbers. Here we can behave as we wish when choosing numbers. Choosing too large numbers makes it difficult to crack the password in encryption and decryption processes. In other words, we can create ASCII Character Codes in infinitely different ways, consisting of 10 numbers.

Example 2: Let's write the letter "A" with ASCII Character Code 65 as 10 numbers.

1741 , -1917 , 511 , 112648, -5099, -75896, 199, 48611, -90159, 9426

We can choose these numbers ourselves as we wish. The sum of these numbers is 65, which is the code for the letter A. When choosing numbers, they can be chosen as fractions or as radicals. In short, any type can be chosen to be different from zero. It can actually be used at zero. However, the use of two zeros consecutively was not desired, as it would mean the line passing through the origin, so it would not be easy.

3.3. Specifying Numbers for the Key

When generating the key, 10 random numbers are selected according to the 10 numbers corresponding to the ASCII Character code. When selecting these numbers, the mutual numbers should not be the same. Because if the numbers are the same, the slope for the chosen binaries will be zero or undefined. Encryption is not possible in case of undefined. Encryption becomes very simple if the slope is zero. Apart from this, there is no limitation in creating keys. Keys can be generated in infinitely different ways.

3.4. Encryption Process

In the encryption process, the numbers of the key will be taken as binaries and will be the first points. The binary states of the 10 numbers that give the code of the character will be the second points. When the third points of the key points are found according to the points of the character code, the encrypted form of the character appears.

3.5. Decryption process

When we apply the rule of finding the third point according to the binaries of the key, the binaries of the encrypted form of a character consisting of 10 numbers will be the 10 number version of the code of the 10 number character. When these 10 numbers are added, the ASCII Character Code of the character will appear and the encryption process will be done.

IV. Conclusion and Discussion

The following results were obtained from this study.

The rule to find the third point from two points in elliptic curves is provided on lines that intersect both axes. In addition, unlike elliptic curves, it wraps around once at three points. Due to this feature, key generation is provided.The reason why ASCII Character Code Table is used in the encryption algorithm is to be used worldwide when the software is made. The ASCII Character Code of each character to be encrypted can be found as the sum of 10 numbers. Thanks to this feature, it allows a character code to be written in infinitely different ways. These 10 numbers can be written in fractions if desired, or they can be written as irrational numbers. After all, it is enough to give the totals character code.If we want to write the character code not as 10 numbers but with the numbers of the Binary system, we need to use 256 numbers or more. Because ASCII Character Code is 255 at most. Therefore, if only 1 is used, 255 digits are required. When done in this way, since the number of zeros will be high for small codes, when we use a key, the encryption can be decrypted because the lines passing through the origin will be more. In order to overcome this problem, if we write the two consecutive numbers as 01, 10, 11 instead of 00, we will overcome the problem. My advice is not to use the binary system's digits.When the numbers to be selected while creating the key are matched with the numbers coming from the character code, it provides infinite selection right provided that they are not the same. Numbers in the key can be either fractional or irrational.The most important rule in this encryption is that the key of the person who will send the message should find the third point according to the character code. Not if the opposite is done. Let's explain it as follows. Let the key of the message sender be point A, and let B point be the code of the character to be sent. Let the third point of point A with respect to point B be point C. C point will be

encrypted text. The point that comes from the rule of finding the third point with respect to point A of point C will be point B. Point B was the point to be encrypted anyway. It was created using the feature of rewinding at three points in line equations.

A → B → C → A → B
As you can see, it wraps around in three points.If point B to be encrypted in encryption was encrypted with respect to point A, which is the Key;
It would be B → A → C → B → A. In this case, the essentially required point B could not be obtained. One of the most important features of this algorithm is that the character code to be encrypted can be written as the sum of as many numbers as desired. It can also be encrypted by creating 250 numbers, provided that they give the total character code. This number of numbers can be set infinitely, making it difficult to crack the encryption and decryption process as the length of the key increases. One of the most important features that make this algorithm secure is that the correct equation in both pairs will be different, so the slope will be different. Therefore, a person who wants to analyze has only one point. Passing through a point will have to be infinitely correct and will have to process forever. If we create the key from 3000 numbers, it will try to find the equation of 1500 lines.

References

[1] Akben, B., Subaşı, A. (2005). Comparison of RSA and Elliptic Curve Algorithm, Kahramanmaraş: Journal of the Faculty of Science and Engineering [2] Levi, A. &Özcan, M. (2010). Why is Public Key-Based Encryption Difficult ?, Istanbul: Sabancı University Faculty of Engineering and Natural Sciences
[3] Kodaz, H. &Botsalı, F. (2010). Comparison of Symmetric and Asymmetric Encryption Algorithms Konya: SelçukTeknikDergisi
[4] Demirci, S. &Şentürk, S. (2015). Digits of Numbers, Basis Arithmetic, Istanbul: Cartesian Publications
[5] Afacan, E. (2017). Introduction to Cryptography, Encryption Theory, Ankara: Epos Publications
[6] Ural, N. &Örenç, Ö. (2014) Encryption and Decryption Methods, Ankara: Pusula Publishing
[7] Yücelen, M. & Baykal, A. &Çoskun, C. (2017) Application of elliptic curve algorithm in cryptology, Diyarbakır: Dicle University Faculty of Engineering journal