International Mathematical Forum, Vol. 6, 2011, no. 49, 2409 - 2418

An Application of Discrete Algorithms in Asymmetric Cryptography

F. Amounas[1] **and E. H. El Kinani**[2]

[1] Informatics Department, Faculty of Sciences and Technics
Moulay Ismaïl University
Box 509 Errachidia, Morocco

[2] Mathematical Department, Faculty of Sciences and Technics
Moulay Ismaïl University
Box 509 Errachidia, Morocco
elkinani_67@yahoo.com

A. Chillali

Mathematical Department, Faculty of Sciences and Technics
Sidi Mohammed Ben Abdelalh University
Box 2202 Fès, Morocco

Abstract

In this paper we propose an application of public key distribution based on the security depending on the difficulty of elliptic curve discrete logarithm problem. More precisely, we propose an example of Elgamal encryption cryptosystem on the elliptic curve given by the equation: $y^2 = x^3 + 70x + 57$[73].

Mathematics Subject Classification: 11G07, 94A60, 11T71, 14G50, 68P25

Keywords: Cryptography, elliptic curve, discrete logarithm, elliptic curve cryptosystem

1 Introduction

Elliptic curves are fundamental objects in a large part of mathematics they are very interesting because their study involves several fields of mathematics. The study of elliptic curves has a long history and still there are many

unsolved problems. In the last decade the application of the elliptic curves in cryptography have been attracting increased attention of many scientists [see e.g [1, 2]] because they have opened a wealth possibilities in terms of security. The elliptic curve cryptosystem (ECC), which was originally proposed by Niel Koblitz and Victor Miller in 1985 [2], is seen as a serious alternative to RSA because there key size is much shorter than that of RSA and Elgamal [3]. The application of elliptic curves to the field of cryptography has been relatively recent, numerous cryptosystems base their security on the difficulty of solving the discrete logarithm problem. The comparison of two cryptosystems using public key cryptosystem RSA and the cryptosystem based on elliptic curve is done in [4]. Recently the author [5], describes the first practical experiments employing cryptography based on elliptic curves. In [6] a new public key cryptosystem (analogue of RSA) based on elliptic curves over the ring Z_n is described. Indeed the security of the RSA and Elgamal cryptosystems [3, 9] is generally equated to the difficulty of integer factorization and that of the computation of discrete logarithms in finite fields respectively. This paper describes the public-key cryptosystems based on the elliptic curve discrete logarithm problem. In particular, here we propose an example of Elgamal encryption cryptosystem based into an elliptic curve given by the following equation: $y^2 = x^3 + 70x + 57$[73]. The paper is organized as follows, first we give some preliminary notes connected with the elliptic curves, the rules for addition on its points and the discrete logarithm problem. Section 3, is devoted to the main results, first we give the table of the curve points, the corresponding alphabetical symbols and the corresponding code, then we follow the Elgamal cryptosystem to encrypt and to decrypt the message which Alice wishes to send Bob.

2 Preliminary Notes

In this section, we introduce some basics notions connected with elliptic curves. For more details on the theory of elliptic curves, we refer interested reader to [7, 8].

2.1 Definition of the Elliptic Curves

Here we begin with the definition of an elliptic curve. Let $\mathbf{K}$ be a field. For example, $\mathbf{K}$ can be the finite (extension) field $\mathbf{F_{q^r}}$ of $\mathbf{F_q}$, the prime field $\mathbf{Z_p}$ where p is a (large) prime, the field $\mathbf{R}$ of real numbers, the field $\mathbf{Q}$ of rational numbers, or the field $\mathbf{C}$ of complex numbers.

Definition 2.1 *An elliptic curve over a field* $\mathbf{K}$ *is the set of points satisfying*

the Weierstrass equation:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \tag{1}$$

and also an element denoted O and called the point at infinity, where $a_1, a_3, a_2, a_4, a_6 \in \mathbf{K}$.
The elliptic curve E over $\mathbf{K}$ *is denoted* $E(\mathbf{K})$ *and the number of points on E is denoted card* $E(\mathbf{K})$.

Remarks
1-For fields of various characteristics, the Weierstrass equation Eq.(1) can be transformed into different forms by a linear change of variables.
2-For the homogeneous, so called also projective, coordinate system, $(x, y) = (\frac{X}{Z}, \frac{Y}{Z})$, the equation (1) determining an elliptic curve point takes the following form :

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3. \tag{2}$$

The point at infinity is the collection of points on the projective plane for which $Z = 0$. The point at infinity is the point of intersection where the y-axis and the line at infinity meet. More precisely, the point at infinity is $(0, 1, 0)$ in the projective plane (the equivalence class with $X = Z = 0$). An elliptic curve E over a finite field $\mathbf{K}$ can be made into an abelian group by defining an additive operation on its points.

2.2 The Rules for Addition

Theorem 2.2 *For each three points* $M(x_1, y_1), N(x_2, y_2)$ *and* $R(x_3, y_3)$ *of the elliptic curves defined in Eq(2) such that* $R = M + N$. *Then R is given by:*
i)$R = O$ *for* $x_1 = x_2$ *and* $y_2 = -y_1 - a_1x_1 - a_3$
ii)$x_3 = t^2 + a_1t - a_2 - x_1 - x_2$ *and* $y_3 = -(t + a_1)x_3 - s - a_3$
with

$$t = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1}, \text{ if } M \neq N \\ \\ \frac{3x_1^2 + 2a_1x_1 + a_4 - a_1y_1}{2y_1 + a_1x_1 + a_3}, \text{ if } M = N \end{cases}$$

and

$$s = \begin{cases} \frac{y_1x_2 - y_2x_1}{x_2 - x_1}, \text{ if } M \neq N \\ \\ \frac{-x_1^3 + a_4x_1 + 2a_6 - a_3y_1}{2y_1 + a_1x_1 + a_3}, \text{ if } M = N \end{cases}$$

The addition operation defined above turns $E(\mathbf{K})$ *into an abelian group that has O as the identity element.*

2.3 The Discrete Logarithm Problem

Recall that the discrete logarithm problem (LDP) for some group G, is to find an integer p such that $pg_1 = g_2$ (where $g_1, g_2 \in G$). Analogously and since an elliptic curve $E(\mathbf{K})$ is made into an abelian group by an additive operation. In the elliptic curve discrete logarithm problem (EDLP) we solve for an integer x such that $x\alpha = \beta$ given $\alpha, \beta \in E(\mathbf{K})$. The security of ECC (Elliptic Curve Cryptosystem) depends on the difficulty of elliptic curve discrete logarithm problem. In fact for a given two points on $E(\mathbf{K})$, it is computationally infeasible to solve the corresponding elliptic curve discrete logarithm problem. The elliptic curve cryptosystems described in the next section is dependent on the presumed intractability of the EDLP.

3 Main Results

In this section, we present a our main result. First consider the elliptic curve c given by the Weierstrass equation:

$$Y^2 = x^3 + 70x + 57[73]. \tag{3}$$

The following table gives the code of the curves points, here the choosing curve contains 74 points, then if P is the generator point of the group. It is the point witch represents the letter a, as well as $2P$ represents the letter b,..., $74P$ represents '?'

curve point	corresponding code	alphabetical corresponding symbol
$[3, 41]$	000001101010010000001	a
$[66, 10]$	100001000010100000001	b
$[45, 4]$	010110100001000000001	c
$[60, 4]$	011110000001000000001	d
$[47, 58]$	010111101110100000001	e
$[21, 35]$	001010101000110000001	f
$[41, 69]$	010100110001010000001	g
$[53, 72]$	011010110010000000001	h
$[42, 56]$	010101001110000000001	i
$[64, 31]$	100000000111110000001	j
$[29, 59]$	001110101110110000001	k
$[35, 66]$	010001110000100000001	l
$[19, 56]$	001001101110000000001	m
$[63, 67]$	011111110000110000001	n
$[11, 48]$	000101101100000000001	o
$[13, 5]$	000110100001010000001	p
$[32, 5]$	010000000001010000001	q
$[26, 53]$	001101001101010000001	r
$[52, 35]$	011010001000110000001	s
$[50, 2]$	011001000000100000001	t
$[4, 67]$	000010010000110000001	u
$[12, 17]$	000110000100010000001	v
$[57, 30]$	011100100111100000001	w

curve point	corresponding code	alphabetical corresponding symbol
$[1, 37]$	000000101001010000001	x
$[0, 38]$	000000001001100000001	y
$[71, 37]$	100011101001010000001	z
$[23, 16]$	001011100100000000001	A
$[44, 65]$	010110010000010000001	B
$[22, 28]$	001011000111000000001	C
$[24, 31]$	001100000111110000001	D
$[55, 22]$	011011100101100000001	E
$[38, 49]$	010011001100010000001	F
$[28, 68]$	001110010001000000001	G
$[58, 31]$	011101000111110000001	H
$[6, 6]$	000011000001100000001	I
$[46, 47]$	010111001011110000001	J
$[62, 0]$	011111000000000000001	K
$[46, 26]$	010111000110100000001	L
$[6, 67]$	000011010000110000001	M
$[58, 42]$	011101001010100000001	N
$[28, 5]$	001110000001010000001	O
$[38, 24]$	010011000110000000001	P
$[55, 51]$	011011101100110000001	Q
$[24, 42]$	001100001010100000001	R
$[22, 45]$	001011001011010000001	S
$[44, 8]$	010110000010000000001	T
$[23, 57]$	001011101110010000001	U
$[71, 36]$	100011101001000000001	V
$[0, 35]$	000000001000110000001	W
$[1, 36]$	000001010010000000001	X
$[57, 43]$	011100101010110000001	Y
$[12, 56]$	000110001110000000001	Z
$[4, 6]$	000010000001100000001	0
$[50, 71]$	011001010001110000001	1
$[52, 38]$	011010001001100000001	2
$[26, 20]$	001101000101000000001	3
$[32, 68]$	010000010001000000001	4

curve point	corresponding code	alphabetical corresponding symbol
$[13, 68]$	000110110001000000001	5
$[11, 25]$	000110110001000000001	6
$[63, 6]$	011111100001100000001	7
$[19, 17]$	001001100100010000001	8
$[35, 7]$	001001100100010000001	9
$[64, 42]$	010001100001110000001	/
$[64, 42]$	001110100011100000001	@
$[42, 17]$	100000001010100000001	*é*
$[53, 1]$	010101000100010000001	*è*
$[41, 4]$	011010100000010000001	*ù*
$[21, 38]$	010100100001000000001	*à*
$[47, 15]$	001010101001100000001	.
$[60, 69]$	010111100011110000001	,
$[45, 69]$	011110010001010000001	;
$[66, 63]$	010110110001010000001	+
$[3, 32]$	100001001111110000001	−
O	000000000000010000001	?

Table.1 *giving the curves points, corresponding codes and the corresponding alphabetical symbol.*

Here we follow Elgamal cryptosystem [3], first recall that the Elgamal cryptosystem consist in the following steps:
Suppose that we have some elliptic curve E defined over a finite field F_q and that E and a point $P \in E$ are publicly known, as is the embedding system $m \longmapsto P_m$; which imbed plain text on an elliptic curve E. Then, when Alice wants to communicate secretly with Bob, they proceed thus:

step 1. Bob chooses a random integer a, and publishes the point aP (while a remains secret).

step 2. Alice chooses her own random integer l and sends the pair of points $(lP, P_i + l(aP))$ to Bob (while a remains secret).

step 3. To decrypt the message, Bob calculates $a(lP)$ from the first part of the pair, then subtracts it from the second part to obtain $P_i + l(aP) - a(lP) = P_i + laP - laP = P_i$, and then reverses the embedding to get back the message.

Here in our case Alice wishes to send a message '*cryptography*' to Bob. First, she imbeds the message '*cryptography*' onto the elliptic curve E, i.e. she

represents the plain text '*cryptography*' as a set of points $P_i \in E$ (where i take the alphabetical letter of plain text '*cryptography*') .

In our case we have $K = (P, a, R)$ with $P = [3, 41], a = 41, R = aP$.
and we take $l \in 0, 1, 2....., 73$ random, $l = 33$ the encryption function is:

$$e_K(P_i) = (Y_i, Z_i)$$

with $Y_i = Y = 33P = [28, 68]$; (which is fixed for each i)
and $Z_i = 33R + P_i = [4, 67] + P_i$

The cipher text is given in the following table

plain text	the point P_i	$e_K(P_i)$	cipher text
C	$[22, 28]$	$([28, 68], [1, 36])$	GX
r	$[26, 53]$	$([28, 68], [6, 67])$	GM
y	$[0, 38]$	$([28, 68], [44, 8])$	GT
p	$[13, 5]$	$([28, 68], [62, 0])$	GK
t	$[50, 2]$	$([28, 68], [28, 5])$	GO
o	$[11, 48]$	$([28, 68], [46, 47])$	GJ
g	$[41, 69]$	$([28, 68], [44, 65])$	GB
r	$[26, 53]$	$([28, 68], [6, 67])$	GM
a	$[3, 41]$	$([28, 68], [12, 17])$	Gv
p	$[13, 5]$	$([28, 68], [62, 0])$	GK
h	$[53, 72]$	$([28, 68], [22, 28])$	GC
y	$[0, 38]$	$([28, 68], [44, 8])$	GT

Table.2: *the embedding of the plain text into elliptic curve, the encryption function and the corresponding cipher text*

Hence the message '*Cryptography*' is transformed into the message 'GXGMGTGKGOGJGBGMGVGKGCGT', then from the table.1, the message becomes a series of codes these :

00111001000100000000100000101001000000001001110010001000000001

00001101000011000000100111001000100000000101011000001000000001

00111001000100000000101111100000000000000100111001000100000001

00111000000101000000100111001000100000000101011100101111000001

00111001000100000000101011001000001000000100111001000100000001

00001101000011000000100111001000100000000100011000010001000001

00111001000100000000101111100000000000000100111001000100000000 1

00101100011100000000100111001000100000000101011000001000000000 1

When Bob received the above series of bits, he transform it into pair of points (Y_i, Z_i) and compute the corresponding decryption function:

$$d_K(Y_i, Z_i) = Z_i - aY_i = [4, 67] + P_i - 41Y_i.$$

After decrypting the received message and using the table.3, we obtain the plain text '*Cryptography*'.

cipher text	the point (Y_i, Z_i)	$d_K(P_i)$	plain text
GX	$([28, 68], [1, 36])$	$[22, 28]$	C
GM	$([28, 68], [6, 67])$	$[26, 53]$	r
GT	$([28, 68], [44, 8])$	$[0, 38]$	y
GK	$([28, 68], [62, 0])$	$[13, 5]$	p
GO	$([28, 68], [28, 5])$	$[50, 2]$	t
GJ	$([28, 68], [46, 47])$	$[11, 48]$	o
GB	$([28, 68], [44, 65])$	$[41, 69]$	g
GM	$([28, 68], [6, 67])$	$[26, 53]$	r
Gv	$([28, 68], [12, 17])$	$[3, 41]$	a
GK	$([28, 68], [62, 0])$	$[13, 5]$	p
GC	$([28, 68], [22, 28])$	$[53, 72]$	h
GT	$([28, 68], [44, 8])$	$[0, 38]$	y

Table.3 : *the cipher text, the corresponding points, the decryption function and the plain text*

4 Conclusion

In this paper, we have proposed an application of public key distribution based on the security depending on the difficulty of elliptic curve discrete logarithm problem. More precisely, we have proposed an example of Elgamal encryption cryptosystem on the elliptic curve given by the following equation: $y^2 = x^3 + 70x + 57$[73].

References

[1] V. S. Miller. Use of Elliptic Curves in Cryptography. Advances in Cryptology CRYPTO'85(1986), pp. 417-426.

[2] N. Koblitz. Elliptic Curve Cryptosystems. Mathematics of Computation, Vol. 48, No. 177 (1987), pp. 203-209.

[3] T.Elgamal, A public key cryptosystem and a signature scheme based on discrete logarithms. IEEE, Transactions on Information Theory, Vol.31(1985), pp.473- 481.

[4] T.E. Rakotondraina., F.Randimbindrainibe, J.Razakarivony. "Performance des crypto systèmes basés sur les courbes elliptiques", ACM, Vol. 21(1978), pp.120-126.

[5] R. Lercier. "Courbes Elliptiques et cryptographie". Numéro 64 dans Revue Scientifique et Technique de la Défense, (2004), pp.59-66. Délégation générale pour l'armement.

[6] N. Demytko. A New Elliptic Curve Based Analogue of RSA. in T. Helleseth, editor, Advances in Cryptology-Eurocrypt'93, Springer-Verlag, New York, (1994), pp. 4049.

[7] J. W. S. Cassels. Lectures on Elliptic Curves. Cambridge University Press, 1991.

[8] A. Atkin and F. Morain. Elliptic curves and primality proving. Mathematics of Computation, Vol. 61, No. 203(1993), pp. 29-68.

[9] M. Saeki. Elliptic curve cryptosystems. M.Sc. thesis, School of Computer Science, McGill University, 1996.

Received: April, 2011