April 1999 Presentation Topic
Cryptography and Elliptic Curves
V. Kumar Murty

Department of Mathematics
University of Toronto

This is a summary of what was presented and discussed at the April 22nd **SIMMER** meeting, along with some problems and questions to think about.

What is Cryptography?

Language is a kind of code. It is a mnemonic for meaning. We use language to communicate meaning. Sometimes, we want to use it so as to include people and reach as many as possible, as for example in advertisements or in political speeches. Sometimes, we want to use it so as to keep a secret and exclude people. Cryptography is the use of language in the second sense. We want only those who belong to our little club (so called authorized people) to be able to understand the meaning.

We can learn an unfamiliar language in many ways, but mostly by exposure to it. This is the idea behind immersion in a language, such as French immersion. It is the same principle in music or dance. What looks at first like meaningless sound or movement slowly becomes meaningful as we expose ourselves to it. The same applies to codes and that is why no code will live forever. People will learn the language in course of time and then we need a new secret language.

Sometimes, we can make a language difficult to understand by placing it in an inaccesible medium. For example, a smart card may contain all sorts of information about the holder. But unless you have a machine that can read the card, you cannot access that information. It is similar to experts in a field using technical jargon to explain things.

The mathematics of cryptography has to do with using numbers as a language whose meaning is difficult to decipher. Some may say that numbers themselves are difficult to decipher and so confusing that no additonal code is necessary! Nevertheless, cryptography looks for ways of expressing information that one wishes to communicate to selected or authorized people.

What are elliptic curves?

They are cubic curves of the form

$$y^2 = x^3 + ax + b$$

such that the cubic polynomial on the right hand side has three distinct roots. For example,

$$y^2 = x(x-1)(x+1)$$

is an elliptic curve, but

$$y^2 = x(x-1)^2$$

is not. The difference between the two is that when there are repeated roots, the curve is essentially a conic. For example, in the above case, making the change of variable

$$w = y/(x-1)$$

the equation becomes

$$x = w^2$$

which is the equation of a parabola. When the roots are distinct, there is no coordinate change that will identify the curve with a conic.

Adding Points on an Elliptic Curve

The special property of elliptic curves is that two points on the curve can be added to get a third point. The set of points forms a group. The identity of the group is the point at "infinity". The addition is defined as follows: three points P, Q and R add to zero: $P + Q + R = 0$ if they lie on a line.

Exercise 1

On the elliptic curve

$$y^2 = x^3 - 36x$$

add the points $P = (-3, 9)$ and $Q = (-2, 8)$.

Elliptic Curves over a Finite Field

We can consider solutions of the equation

$$y^2 = x^3 + ax + b$$

in a finite field. For example, we can consider the solution set to the congruence

$$y^2 \equiv x^3 + ax + b \pmod{p}.$$

Exercise 2 Find the solution set of

$$y^2 \equiv x^3 + x \pmod{7}.$$

Cryptography and Elliptic Curves

Pick an elliptic curve E and a prime p. Let us say that E has N points on it. Let us say that our alphabet consists of the digits $0, 1, 2, 3, 4, 5, 6, 7, 8, 9$ and the letters $A, B, C, \ldots, X, Y, Z$ coded as $10, 11, \ldots, 35$. This converts our message into a series of numbers between 0 and 35. Now choose an auxiliary base parameter, for example $k = 20$. For each number mk (say), take $x = mk + 1$ and try to solve for y. If you can't do it, then try $x = mk + 2$ and then $x = mk + 3$ until you can solve for y. In practice, you will find such a y before you hit $x = mk + k - 1$. Then take the point (x, y). This now converts the number m into a point on the elliptic curve. In this way, the entire message becomes a sequence of points.

On the other hand, if we are given a sequence of points on the curve, to decode it, we consider each point (x, y) and set m to be the greatest integer less than $(x-1)/k$. Then the point (x, y) decodes as the symbol m.

In order to actually carry this out one has to be able to solve the congruence

$$y^2 = a \pmod{p}.$$

There is an algorithm for this, but for tonight we will just use a table.

In actual applications, cryptography using elliptic curves is much more complicated. In fact, what we have discussed above is the "easy" part. One does some more operations on the points constructed so as to make them harder to decipher.

Exercise 3

Consider the elliptic curve

$$y^2 + y \equiv x^3 - x \pmod{751}.$$

This curve has $N = 727$ points. Write the message

STOP007

as a sequence of seven points on the curve. Decode the sequence of points

$$(361, 383), (241, 605), (201, 380), (461, 467), (581, 395)$$

into a reply message.

References

1. Neal Koblitz, *Elliptic Curves and Cryptography*, Springer-Verlag.

2. The site www.certicom.com has really good material on elliptic curves and cryptography, including a tutorial at http://www.certicom.com/ecc/index.htm.