4-11-2011

Elliptic Pairs of Primes in Cryptography and Their Effects on RSA Security

Suzanne Craig
Department of Mathematics, Boise State University

Liljana Babinkostova
Department of Mathematics, Boise State University

Elliptic Pairs of Primes in Cryptography and their effects on RSA security

Suzanne Craig and Liljana Babinkostova, Ph.D.
Boise State University Department of Mathematics

Background and Basic Terminology

Cryptography is a constantly evolving field – elliptic curve groups have been a major part of this field since 1987 when Koblitz and Miller separately proposed their use in cryptosystems such as RSA.

- ❖Elliptic Curve: A curve defined by the equation: $y^2 = x^3 + Ax + B$ where A and B are less than a prime p, and where the discriminant is not equal to zero. We are concerned with the curves where A = 0.
- ❖Elliptic Curve Group (ECG): A group whose elements are defined by the elliptic curve and the operation in question. Elliptic curves naturally qualify as groups due simply to their nature.
- ❖Elliptic Pair of Primes: Two primes (p,q) such that an ECG defined by the following equation $y^2 = x^3 + B \bmod p$ has an order q, and the ECG defined by a different equation mod q has the order p. These pairs are the main topic of our study, and learning more about them and their effects on RSA security is our primary goal.
- ❖Discrete Log Problem (DLP): Solving for x in the equation: $g^x = b$

NOTE: Operations such as addition and multiplication are defined differently when used in terms of an ECG operation. An example can be found below.

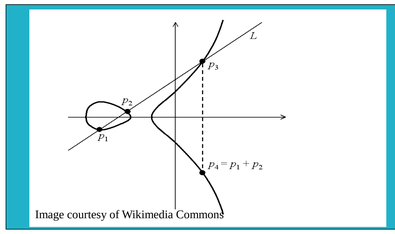


Image courtesy of Wikimedia Commons

The geometric, or graphical, representation of 'addition' of two points on an elliptic curve.

Conjectures

- ❖When the elliptic curve defined by the equation: $y^2 = x^3 + B \bmod p$ has a prime order, then either in all investigated cases or in approximately half the investigated cases we have B primitive root modulo p (the initial prime used to generate the data).
- ❖When the elliptic curve has all investigated cases B primitive root modulo p, the groups have one of two prime orders. When the curve has approximately half the cases B primitive root modulo p, all the relevant groups have an identical group order, which is prime.

Methods

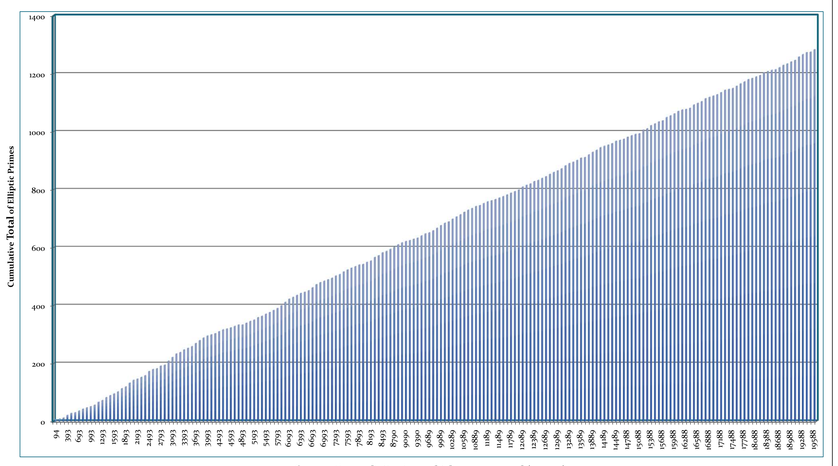
We used a series of MAPLE procedures to collect and analyze data in a series of worksheets, which found the order of the groups and tested if the prime order and the initial prime were an elliptic pair: We also used MAPLE procedures to collect data relevant to our conjectures (listed above) in order to prove or disprove them.

Some Results

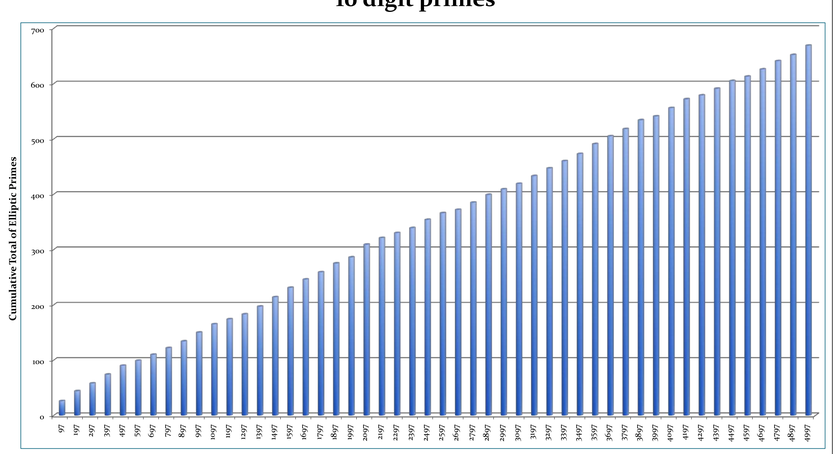
Elliptic Curves of the type $y^2 = x^3 + B$ where B is a primitive root modulo p were surveyed for primes 'p' within certain intervals and if they had prime group order they were counted in order to determine if there was a distribution pattern of prime ordered groups

NOTE: the following graphs only show the 20 digit primes and the 10 digit primes that we surveyed, we actually surveyed 6 digit primes, 10 digit primes, 12-18 digit primes, and 20 digit primes: the patterns that are stated applied to all these intervals of primes, not just 10 and 20 digit primes. Total we surveyed approximately 25,000 primes.

20 digit primes



10 digit primes



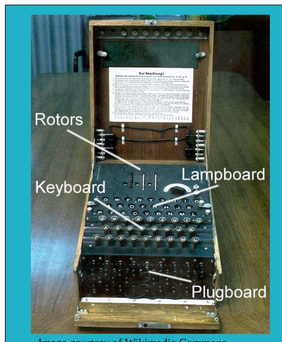


Image courtesy of Wikimedia Commons

One of the infamous Enigma Machines, used in World War II by the Nazis as a rotor cipher machine. Information security no longer relies on manual rotations of keys but on complex computations and highly developed algorithms

Something to think About

Question: What is the probability that the prime order of a group characterized by an equation such that $y^3 = x^3 + B \bmod p$ where B is a primitive root modulo p, has a prime order q, and is an elliptic pair, as earlier defined?

Answer: 100%, or all of them are part of an elliptic pair. This is true for both 10 digit primes and 20 digit primes.

A follow-up question: Are all elliptic pairs from groups of the form $y^2 = x^3 + B$ where B is a primitive root mod p?

Future Work

We plan to continue to work on this project for the rest of the semester as well as over the summer and possibly in the Fall 2011 semester, depending on progress made in the following:

- ❖Further data must be gathered
- ❖Possibly proving/disproving the conjectures mentioned
- ❖Tests using Fermat's Attack and possibly other attacks on RSA cryptosystems that use primes in the key generation algorithm that are an elliptic pair of primes.

Updates on this project will be presented at the semi-annual graduate cryptography conference, BoiseCrypt 2011.

Acknowledgements

Thanks go to Liljana Babinkostova, Ph.D., for serving as a research mentor, the National Science Foundation and the Idaho STEP program for funding this project, as well as Boise State University's Department of Mathematics.