Final Project: Public key cryptography, and its relationship to $\mathbb{Z}_{pq}$, finite fields, and elliptic curves

Written by Jonathan Hanke

February 14, 2005

Abstract

One of the most important applications of number theory (and some would say its only application) is to the art of keeping secrets. Because of the popularity of the internet to send private information (e.g. credit card numbers when buying something online), keeping this information private has become a very important issue. It is surprising how simple the mathematics is behind the most popular (and secure?) encryption schemes, and how the age of modern cryptography was born from a few clever applications of these simple ideas. Your project should explain how some of the most popular encryption schemes work, and analyze their security (both in terms of general time estimates, and special situations/keys to avoid). This will lead you to think about the problems of factoring numbers, finding logarithms mod p, and the basics of elliptic curves. **[3-5]**

Good general references for the arithmetic of elliptic curves are [5], [7]. The topics of factoring and primality testing are the focus of the 2 books [3] and [9], though [9] this is not currently in the Duke library. These are also discussed in [4, Chapter VIII], [5, pp107-118 for ranks for some CM curves, pp148–150 for $\mathbb{Z}_p$ points for some CM curves], [7, pp89–98 for some explicit examples, and especially pp125–138 of Chapter IV for an elliptic curve factoring algorithm]. See also [2, Part III]. An easy computer language to do arbitrary precision integer arithmetic is PYTHON, and some simpl examples are described in [1]. There is also another slightly less friendly program [8] designed specifically for number theory/Elliptic curve computation. Both programs are freely available. There are lots of general crypto refrences online. One "standard" refrence is [6], but there are lots of others. The PGP documentation is particularly friendly.

The following is a rough outline which may be useful in thinking about/organizing your project. If you have any questions about your project and/or readings, feel free to let me know, and we can setup a time to talk about it. Have Fun! =)

1. **Differences between Symmetric/Public key cryptosystems**
2. **Arithmetic in $\mathbb{Z}_p$ and $\mathbb{Z}_{pq}$**
3. **Fast algorithms for exponentiation and inverses**
4. **RSA and factoring**
5. **Diffie-Hellman secret sharing, El Gamal, and discrete logarithms**
6. **Digital signatures, hash functions, and secret splitting**
7. **One-time pads and Shannon's theorem**
8. **PGP and GPG software implementations**
9. **Cryptanalysis and time estimates**
10. **Comments about Elliptic Curves and Cryptography**

References

[1] Computations in number theory using python: A brief introduction.

[2] A. K. Bhandari, D. S. Nagaraj, and B. Ramakrishnan, editors. *Elliptic curves, modular forms and cryptography*, New Delhi, 2003. Hindustan Book Agency.

[3] David M. Bressoud. *Factorization and primality testing.* Undergraduate Texts in Mathematics. Springer-Verlag, New York, 1989.

[4] H. Davenport. *The higher arithmetic.* Cambridge University Press, Cambridge, seventh edition, 1999. An introduction to the theory of numbers, Chapter VIII by J. H. Davenport.

[5] Anthony W. Knapp. *Elliptic curves*, volume 40 of *Mathematical Notes.* Princeton University Press, Princeton, NJ, 1992.

[6] Alfred J. Menezes, Paul C. van Oorschot, and Scott A. Vanstone. *Handbook of applied cryptography.* CRC Press Series on Discrete Mathematics and its Applications. CRC Press, Boca Raton, FL, 1997. With a foreword by Ronald L. Rivest.

[7] Joseph H. Silverman and John Tate. *Rational points on elliptic curves.* Undergraduate Texts in Mathematics. Springer-Verlag, New York, 1992.

[8] The PARI Group, Bordeaux. *PARI/GP, version* 2.1.5, 2004. available from http://pari.math.u-bordeaux.fr/.

[9] Song Y. Yan. *Primality testing and integer factorization in public-key cryptography*, volume 11 of *Advances in Information Security.* Kluwer Academic Publishers, Boston, MA, 2004.