Integer Factorization and Discrete Logarithms

Andrew Odlyzko

AT&T Labs, Florham Park, NJ 07932, USA
amo@research.att.com
http://www.research.att.com/~amo

Abstract. Integer factorization and discrete logarithms have been known for a long time as fundamental problems of computational number theory. The invention of public key cryptography in the 1970s then led to a dramatic increase in their perceived importance. Currently the only widely used and trusted public key cryptosystems rely for their presumed security on the difficulty of these two problems. This makes the complexity of these problems of interest to the wide public, and not just to specialists.

This lecture will present a survey of the state of the art in integer factorization and discrete logarithms. Special attention will be devoted to the rate of progress in both hardware and algorithms. Over the last quarter century, these two factors have contributed about equally to the progress that has been made, and each has stimulated the other. Some projections for the future will also be made.

Most of the material covered in the lecture is available in the survey papers [1,2] and the references listed there.

References

1. A.M. Odlyzko, The future of integer factorization, *CryptoBytes (The technical newsletter of RSA Laboratories)*, 1 (no. 2) (1995), pp. 5–12. Available at http://www.rsa.com/rsalabs/pubs/cryptobytes/ and http://www.research.att.com/~amo.
2. A.M. Odlyzko, Discrete logarithms: The past and the future, *Designs, Codes, and Cryptography* 19 (2000), pp. 129-145. Available at http://www.research.att.com/~amo.

G. Gonnet, D. Panario, and A. Viola (Eds.): LATIN 2000, LNCS 1776, pp. 258–258, 2000.