6[11Yxx, 11Txx, 94Axx, 68P25]—*Cryptography and computational number theory*, Kwok-Yan Lam, Igor Shparlinski, Huaxiong Wang, and Chaoping Xing (Editors), Birkhäuser, Basel, Switzerland, 2001, vii+378 pp., 24 cm, hardcover $109.00

This volume represents the proceedings of the Workshop on Cryptography and Computational Number Theory which was held at the National University of Singapore in November 1999. The book contains thirteen articles classified under computational number theory and fourteen articles classified under cryptography. Some papers are surveys and others present new original results. The reviewer found the surveys by D. R. Kohel on elliptic curves for cryptography, by P. Mihăilescu on testing and proving primality, by C. P. Xing on algebraic-geometry methods for constructing almost perfect sequences, and by M. I. González Vasco and M. Näslund on hard core functions to be particularly interesting and useful.

Harald Niederreiter