



9th Conference for African–American Researchers in the Mathematical Sciences
Purdue University, June 24–27, 2003

TUTORIAL ON ELLIPTIC CURVE CRYPTOGRAPHY

Garikai Campbell
Department of Mathematics
Swarthmore College
kai@swarthmore.edu

Part I: A brief history of cryptography. Just what are elliptic curves and why do they have anything at all to do with cryptography?

Part II: More on: the arithmetic of elliptic curves, elliptic curves over finite fields, elliptic curve cryptography and why one would choose to use elliptic curves at all.

Part III: Challenges, a look ahead and summary.