DEPARTMENT OF MATHEMATICS AND COMPUTER SCIENCE
UNIVERSITY OF SOUTHERN DENMARK, ODENSE

COMPUTER SCIENCE COLLOQUIUM

A Speed-Up Theorem for Cryptosystems

René Peralta
Electrical Engineering and Computer Science Department
University of Wisconsin at Milwaukee

Tuesday, May 11, 1999, at 2:15 PM
The Seminar Room

Abstract: We show that any encryption/decryption system can be converted to an algorithm which uses roughly three machine operations per bit. We prove that our technique yields an encryption/decryption system which is as secure as the original system provided the plaintext has full-entropy. We then show how to remove the full-entropy assumption.

Joan Boyar