Mapping Exponentiation - Montgomery
Author: Peter L. Montgomery
Date: 1987-Jul-31
Keywords: Cryptography, Modular arithmetic
Abstract: Suppose MODPROD(A,B,C,M,R) computes (A*B*C) MOD M, where A, B, C, M, and R are all less than R. Let R = b^k for some b and k. Let M satisfy M*M' = -1 (MOD b), for some M'. Then MODPROD(A,B,C,M,R) can be computed by MODPROD(A,B,C,M,R), M, b, k.