Modular exponentiation: let's say we have [610 mod 3 > unsolvable easily (165 mod 3) (165 mod 3) ) mod 3) ((18 mod 3) (164 mod 3)) wod 3 (15 mod 3) (164 mod 3)) mod 3 (1. (164 mod 3)) mod 3 1. (164 mod 3)) mod 3 (1.1) mod 3 1. 1) mod 3 1 Ans

0

Miller Rabin Primality Test Step1: find n-1 = 2k x m Stepz: Choose a' such that 12a2n-1 Steps: compute bo = am (mod n); ..., b; bo bi-1 (mod n) Result of b. +1 -> Composite ~1 -> Probabably frime. h=561 560 = 14 x35 , K=4, M=35 , a>1 and a<5603) bo = 235 (mod 56.1) exponentiation (useit This is modular bo = +1 (mod 561) -> NO Calculate b1 - bo (mod n) = 263: (mod 561)

b= 1 (mod 581) - comprise. (