Notes 2/29/2016

Benjmain Boudra

February 29, 2016

Contents

1 Show RSA works:

Know: for prime p, any $a \in 1, \ldots, p-1, a^{p-1} = 1$ in Z_p Have:
$n = pq$ (p, q primes)
$\alpha = (p-1) * (q-1)$
ext gcd $g, e) = 1 = sq$
$c = a^e \in Z_n$