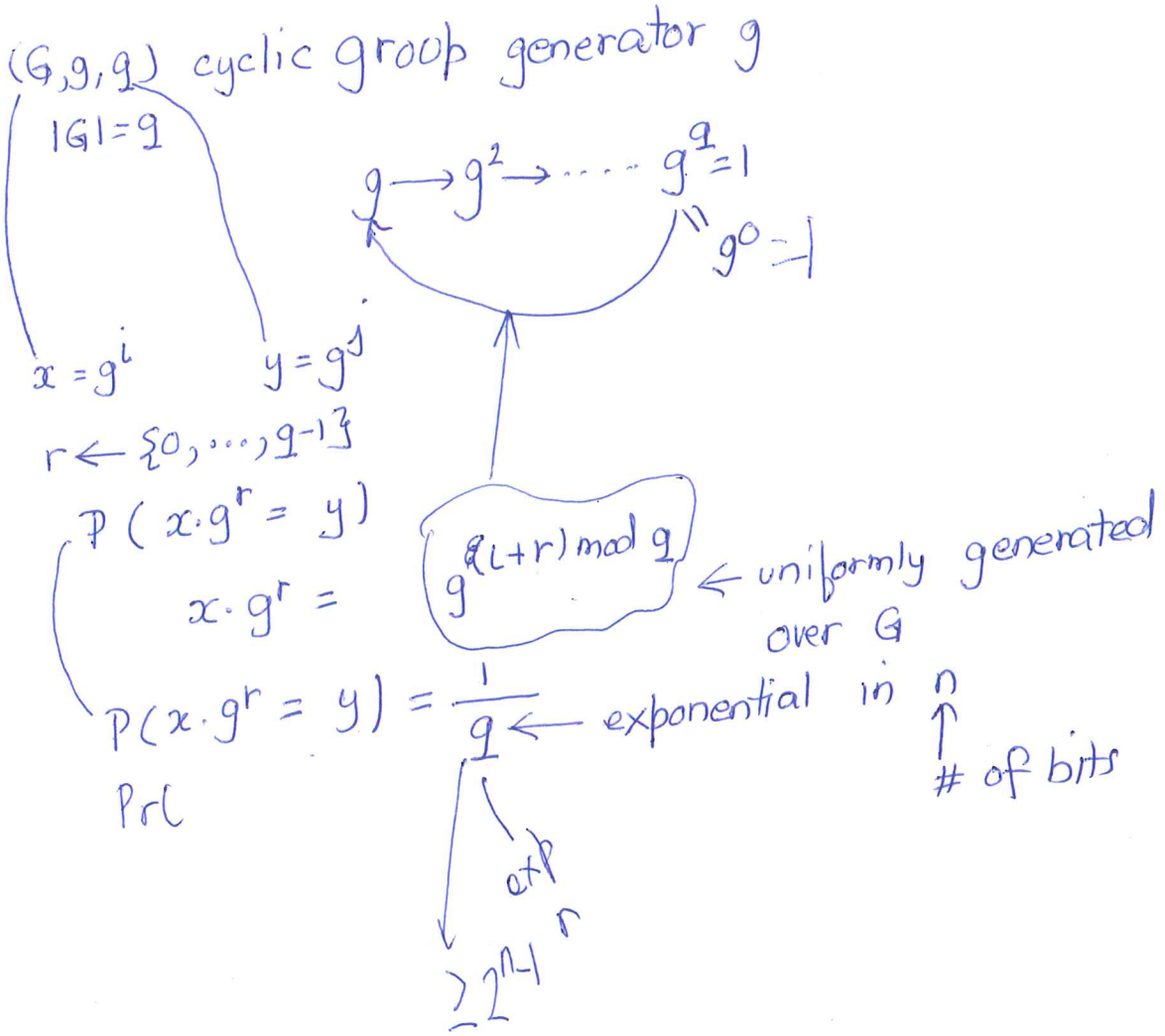
(G, g, q) cyclic group generator g
|G| = q
g → g^2 → ... g^q = 1
g^0 = 1
x = g^i
y = g^j
r ← {0, ..., q-1}
P(x · g^r = y)
x · g^r =
g^((i+r) mod q)
← uniformly generated over G
P(x · g^r = y) = 1/q ← exponential in n
# of bits
Pr(
≥ 2^(n-1)

$x \equiv 3 \pmod 7$

$x \equiv 2 \pmod 9$

$M = 7 \times 9 = 63$

$M_1 = \frac{63}{7} = 9$ $\quad M_2 = \frac{63}{9} = 7$

$N_1 = 4$

9 ~~~~ 2

~~18~~ ~~~~ 4

$9 \cdot 4 \equiv 1 \pmod 7$

$M_1 N_1 \equiv 1 \pmod 7$

9 → 2 → 11 → 4 → 13 → 6 → 15 → 1

7 → 14 → 5 → 12 → 3 → 10 → 1

$7 \cdot 4 \equiv 1 \pmod 9$

$M_2 N_2 \equiv 1 \pmod 9$

$3 M_1 N_1 + 2 M_2 N_2$

$= 3 \times 9 \times 4 + 2 \times 7 \times 4$

$= 108 + 56 = 164$ mod 63 → ~~63~~ 38

$38 \equiv 3 \pmod 7$

$38 \equiv 2 \pmod 9$

check.