1. Alice choose p = 71 and g = 33 (generator Z\*71), x = 62, h = g ^ x mod p = 33 ^ 62 mod 71 = 10 public key(p = 71, g = 33, h = 10)
2. Bob’s message m = 15 random exp r = 31 -> cipher text (g ^ r, h\*m) = 62^-1 mod 71 = 1/62^\*, 62^-1 = 63 mod 71 (62, 18), 62 . 63 = 1 mod 71
3. Alice decrypts (62, 18) -> 18 \* 1/62\* = 18/62^62 mod 71, 18 \* (62^-1) = 18\*63^62 mod 71 = 15