Jake Traut

103134737

CSCI 3104 Algorithms Homework 2

1. Recursive multiplication algorithm input m-bit number x and n-bit number y. There is a total of O(m) bit operation performed each recursive call, and a total of n recursive calls because every call to multiply(x,y) the y is halved, y/2, removing one bit size each time until it gets to 0. This means the total time will be n*O(m) or O(n*m).
2. Compute gcd(770, 546)
    a. Factorization: 770 = 2*5*7*11, 546 = 2*3*7*13, then gcd = 2*7 = 14
    b. Euclid algorithm: gcd(x,y) = gcd(x mod y, y) => Euclid(770, 546) => Euclid(546, 770 mod 546) => Euclid(546, 224) => Euclid(224, 546 mod 224) => Euclid(224, 98) => Euclid(98, 224 mod 98) => Euclid(98, 28) => Euclid(28, 98 mod 28) => Euclid(28, 14) => Euclid(14, 28 mod 14) => Euclid(14, 0) => gcd = 14
    c. Extended Euclid algorithm: d = gcd(a, b) if d = ax + by => d = ay' + b(x' - $\lfloor a/b \rfloor$ y') => gcd(770, 546) = 770(1) + 546(0) = 770 return (1, 0, 770) => 770(0) + 546(1) = 546 return (0, 1, 546) => 770(1) + 546(0-1*1) = 224 return (1, -1, 224) => 770(0-(2*1)) + 546(1-(2*-1) = 98 return (-2, 3, 98) => 770(1-(2*-2)) + 546(-1-(2*3)) = 28 return (5, -7, 28) => 770(-2-(3*5)) + 546(3-(3*-7)) = 14 return (-17, 24, 14) => 770(5-(2*-17)) + 546(-7-(2*24)) = 0 return (39, -55, 0) thus answer is last non-zero step for d which is (x, y, d) = (-17, 24, 14).
3. Modulo: 7^7293 (mod 342) = (7^1 * 7^4 * 7^8 * 7^16 * 7^32 * 7^64 * 7^1024 * 7^2048 * 7^4096) mod 342 => (7^1 mod 342 * 7^4 mod 342 * 7^8 mod 342 * 7^16 mod 342 * 7^32 mod 342 * 7^64 mod 342 * 7^1024 mod 342 * 7^2048 mod 342 * 7^4096 mod 342) mod 342 => (7 * 7 * 49 * 7 * 49 * 7 * 7 * 49 * 7) mod 342 => (13841287201) mod 342 = 1

    Note: powers of 2 for 7^(2x) mod 342 switch between remainder 49 and remainder 7

4. Python RSA cryptography runtimes

    p = 3911 q = 2383
    for n = 9319913
    - RSA Key generator runtime = 0.001083
    - Encryption runtime = 49.427872
    - Decryption runtime = 66.316492

    p = 3167 q = 2411
    for n = 7635637
    - RSA Key generator runtime = 0.001667
    - Encryption runtime = 36.969782
    - Decryption runtime = 34.285652

p = 4787 q = 6449
n = 30871363

- RSA Key generator runtime = 0.000173
- Encryption runtime = 84.424032
- Decryption runtime = 121.129739