4CR3 A3
zhanz479

1.

a.

Euler’s theorem states $a^{\varphi(m)} \equiv 1 \pmod{m}$

The inverse of a modulo m is some number x such that $ax \equiv 1 \pmod{m}$.

From the above equation, we can get $a^1 a^{\varphi(m)-1} \equiv 1 \pmod{m}$, therefore $x = a^{\varphi(m)-1}$.

φ(m) is calculable. We can subtract 1 from that to get x.

Thus, the inverse of a modulo m is $a^{\varphi(m)-1}$

Therefore, we have shown how to find the inverse of a modulo m using Euler’s theorem.

b.

The output of the extended euclidean algorithm on a and m is two integers x and y, such that ax + my = gcd(a,m). Since the gcd of a and m is 1, we have ax + my = 1. If we take this equation modulo m, then we would have: ax = 1 (mod m). This is the inverse of a modulo m by definition. Therefore, we have found the inverse using the extended euclidean algorithm.

c.

a^{-1} mod m is
455849832448654918145271645198762680484609121155948527718155116360107376403525283213075123888664381192832794777034012202625978250778619258394374862217

The extended euclidean algorithm took 0.23440003860741854 milliseconds.

The euler’s theorem algorithm took 3.292199980933219

2.

a.

If the plaintext x is small and the public exponent e is also small, it is possible for x^e, the ciphertext, to be smaller than n, meaning it is not affected by the modulo n operation in the RSA encryption scheme, $y = x^e \pmod{n}$, leaving the plaintext to be $y = x^e$. This would mean that using the public key (n, e) and a found ciphertext, Trudy can compute the e-th root of y to find x. This means they have broken the encryption scheme without the private key. Otherwise, it might also be computationally feasible for Trudy to keep encrypting all the possible values of x until they get a matching ciphertext. From the start, Trudy would know the public key (n, e), and the ciphertext. Trudy can keep generating x’s and computing x^e and see if x^e matches the ciphertext. If it does, that means Trudy has found x, and has broken the encryption.

b.

The plaintext corresponding to the given ciphertext is: x = 63287374328731

3.

In the given situation, Trudy knows:

Bob’s public key: (n, e_1)

Alex’s public key: (n, e_2)
Bob’s cipher text: $y_1 = x^{e}{}_1$ (mod n)
Alex’s cipher text: $y_2 = x^{e}{}_2$ (mod n)

Given that $\gcd(e_1, e_2) = 1$, using the extended euclidean algorithm, Trudy can find two numbers a and b, such that $ae_1 + be_2 = 1$. If we find the values $s = y_1^a$ and $t = y_2^b$, we can multiply them together:

$$st = y_1^a y_2^b = x^{e_1 a} x^{e_2 b} = x^{e_1 a + e_2 b} = x^1 \ (mod\, n)$$

Since we know y_1, y_2, n, e_1, e_2, a, and b, we are able to calculate x, the plaintext message that Alice sent to Bob and Alex.