Adam Livingston

5 Apr 2022

BASV 376 Mathematics for Applied Technology

Assistant Professor Emily Carroll

Practical Exercise 3

**Practical Exercise Option 2**

Given:

Suppose Emily wants to use RSA to communicate securely with her brother Dan. However, she made a poor choice of p and q. She constructs n and chooses e accordingly.

𝑛 = 𝑝 ∗ 𝑞 = 65 and

𝜙(𝑛) = (𝑝 − 1) ∗ (𝑞 − 1).

𝑒 = 11 [this is a good choice for 𝑒, since 𝐺𝐶𝐷(11,𝜙(𝑛)) = 1]

She publishes (e, n) as her public key. Dan uses it to encrypt a secret message and sends it to her.

The ciphertext is 𝐶 = 𝑀e 𝑚𝑜𝑑 𝑛 = 21.

**Compute:**

***a. Find 𝑝, 𝑞, and 𝜙(𝑛). Explain briefly how you found 𝑝 and 𝑞.***

First, find factors of p\*q = 65

1 \* 65

5 \* 13

Therefore, we know that there are only two possibilities for 𝜙(𝑛):

(13 – 1) \* (5 – 1)

Or

(65 – 1) \* (1 – 1)

Since the second equation will result in a product of 0, we know that the only possibility for 𝜙(𝑛) is (13 – 1) \* (5 – 1) = (12)(4) = 48

To sanity-check this, let’s determine GCD(48, 11), which should equal 1:

a = bq + r

a = b(q) + r

48 = 4(11) + 4

11 = 2(4) + 3

**4 = 1(3) + 1 GCD = 1**

3 = 3(1) + 0

*b. Use the Extended Euclidean Algorithm to construct 11𝑥 + (𝜙(𝑛))𝑦 = 1.*

Substituted Equation with 𝜙(𝑛): 1 = 11x + 48y

1 = 4 – 1(3)

1 = 4 – 1(11 – 2(4)) Substitute [3 = 11 – 2(4)]

1 = 4 – 1(11) + 2(4) Distribute -1

1 = 3(4) – 1(11) Combine like terms

1 = 3(48 – 4(11)) – 1(11) Substitute [4 = 48 – 4(11)]

1 = 3(48) – 12(11) – 1(11) Distribute 3

1 = 3(48) – 13(11) Combine like terms

*c. Using your answer from part b, find the value of 𝑑:*

*if 𝑥 > 0, let 𝑑 = 𝑥. If 𝑥 < 0, let 𝑑 = 𝑥 + 𝜙(𝑛).*

Since x = -13, then x < 0 therefore,

d = x + 𝜙(𝑛)

d = -13 + 48 Substitute

d = 48 – 13 Rearrange

d = 35 Calculate

*d. Using 𝑑, decrypt the ciphertext by performing 𝐶e 𝑚𝑜𝑑 𝑛 = 𝑀.*

First, find M:

Ciphertext: 𝐶 = 𝑀e 𝑚𝑜𝑑 𝑛 = 21.

C = 21

n = p \* q = 65

e = 11

𝐶e 𝑚𝑜𝑑 𝑛 = 𝑀 Equation

2111 mod 65 = M Substitute with known values

M = 31 Calculate with wolfram

Calculate for C

C = 𝑀e 𝑚𝑜𝑑 𝑛

21 = 3111 𝑚𝑜𝑑 65 Substitute

21 = 21 🗸 Calculate with wolfram