2. RSA

a. Encrypt the message m = 12 with the public key, showing your work.

Computes the encrypted message: c = m^(e) mod n

c = 12^3 mod 55 = 23

b. Find the unique value $0 \le d < 40$ such that $d * e = 1 \bmod 40$

We know that:
φ(n) = (5 − 1)(11 − 1) = 40
e = 3
Compute d such that ed = 1 mod φ(n)
We can easily compute that d = 27
Check:
ed = 1 mod φ(n)
3*27 = 81 = 1 mod 40

c. Decrypt the message m = 3 using the private key pair (d, n) as calculated in the previous step, using the modulo trick, showing your work

Decrypted_message = m^(d) mod n
= 3^27 mod 55 = 27^9 mod 55

Using the trick (a*b) mod n = [(a mod n)* (b mod n)] mod n
We can easily calculate the following without calculator

27^2 mod 55 = 27 * 27 mod 55 = 14
27^4 mod 55 = (27^2 mod 55 * 27^2 mod 55) mod 55 = 14^2 mod 55 = 31
27^8 mod 55 = (27*4 mod 55 * 27^4 mod 55) mod 55 = 31^2 mod 55 = 26

Now we know that: (by plugging 27^8 mod 55)
27^9 mod 55 = (27^8 mod 55 * 27 mod 55) mod 55 = 26*27 mod 55 = 42
Using this method, we avoid to do complicated computations and avoid to store large numbers.