**1. Notation for Generating RSA Key Pair, Encryption, and Decryption**

**Key Generation:**

1. Choose two distinct prime numbers ppp and qqq.
2. Compute n=p×qn = p \times qn=p×q.
3. Compute ϕ(n)=(p−1)×(q−1)\phi(n) = (p - 1) \times (q - 1)ϕ(n)=(p−1)×(q−1).
4. Choose an integer eee such that 1<e<ϕ(n)1 < e < \phi(n)1<e<ϕ(n) and gcd⁡(e,ϕ(n))=1\gcd(e, \phi(n)) = 1gcd(e,ϕ(n))=1.
5. Compute ddd such that d≡e−1mod  ϕ(n)d \equiv e^{-1} \mod \phi(n)d≡e−1modϕ(n) (i.e., ddd is the modular multiplicative inverse of eee modulo ϕ(n)\phi(n)ϕ(n)).

The public key is (e,n)(e, n)(e,n) and the private key is (d,n)(d, n)(d,n).

**Encryption:** To encrypt a plaintext message mmm: c≡memod  nc \equiv m^e \mod nc≡memodn where ccc is the ciphertext.

**Decryption:** To decrypt a ciphertext ccc: m≡cdmod  nm \equiv c^d \mod nm≡cdmodn where mmm is the original plaintext message.

**2. Decoding in RSA**

Given the private RSA key (7,11)(7, 11)(7,11), let's decode the ciphertext symbols 5, 9, and 3.

Here, the modulus nnn is 11 and the private exponent ddd is 7.

For each ciphertext symbol ccc: m≡cdmod  nm \equiv c^d \mod nm≡cdmodn

* For c=5c = 5c=5: m≡57mod  11m \equiv 5^7 \mod 11m≡57mod11 57=781255^7 = 7812557=78125 78125mod  11=478125 \mod 11 = 478125mod11=4 So, m=4m = 4m=4.
* For c=9c = 9c=9: m≡97mod  11m \equiv 9^7 \mod 11m≡97mod11 97=47829699^7 = 478296997=4782969 4782969mod  11=34782969 \mod 11 = 34782969mod11=3 So, m=3m = 3m=3.
* For c=3c = 3c=3: m≡37mod  11m \equiv 3^7 \mod 11m≡37mod11 37=21873^7 =
* 218737=2187 2187mod  11=12187 \mod 11 = 12187mod11=1 So, m=1m = 1m=1.

**3. Matching RSA Keys**

To find which private RSA key matches the public key (5,91)(5, 91)(5,91), we need to determine which private key (d,91)(d, 91)(d,91) satisfies d×e≡1mod  ϕ(n)d \times e \equiv 1 \mod \phi(n)d×e≡1modϕ(n), where e=5e = 5e=5 and n=91n = 91n=91.

First, factorize n=91n = 91n=91: 91=7×1391 = 7 \times 1391=7×13 ϕ(91)=(7−1)×(13−1)=6×12=72\phi(91) = (7 - 1) \times (13 - 1) = 6 \times 12 = 72ϕ(91)=(7−1)×(13−1)=6×12=72

We need ddd such that: d×5≡1mod  72d \times 5 \equiv 1 \mod 72d×5≡1mod72 Let's check each private key:

* d=19d = 19d=19: 19×5=9519 \times 5 = 9519×5=95 95mod  72=2395 \mod 72 = 2395mod72=23 Not a match.
* d=24d = 24d=24: 24×5=12024 \times 5 = 12024×5=120 120mod  72=48120 \mod 72 = 48120mod72=48 Not a match.
* d=29d = 29d=29: 29×5=14529 \times 5 = 14529×5=145 145mod  72=1145 \mod 72 = 1145mod72=1 This is a match.

Therefore, the matching private key is (29,91)(29, 91)(29,91).

**4. Generating my Own RSA Key Pair**

Let's generate an RSA key pair with primes in the range from 20 to 100.

1. Choose two primes ppp and qqq: Let's choose p=61p = 61p=61 and q=53q = 53q=53.
2. Compute n=p×qn = p \times qn=p×q: n=61×53=3233n = 61 \times 53 = 3233n=61×53=3233
3. Compute ϕ(n)=(p−1)×(q−1)\phi(n) = (p - 1) \times (q - 1)ϕ(n)=(p−1)×(q−1): ϕ(n)=60×52=3120\phi(n) = 60 \times 52 = 3120ϕ(n)=60×52=3120
4. Choose eee such that 1<e<ϕ(n)1 < e < \phi(n)1<e<ϕ(n) and gcd⁡(e,ϕ(n))=1\gcd(e, \phi(n)) = 1gcd(e,ϕ(n))=1: Let's choose e=17e = 17e=17.
5. Compute ddd such that d≡e−1mod  ϕ(n)d \equiv e^{-1} \mod \phi(n)d≡e−1modϕ(n): Use the Extended Euclidean Algorithm to find ddd: d×17≡1mod  3120d \times 17 \equiv 1 \mod 3120d×17≡1mod3120 The solution is d=2753d = 2753d=2753.

So, the public key is (17,3233)(17, 3233)(17,3233) and the private key is (2753,3233)(2753, 3233)(2753,3233).

**Testing the key pair:**

Let's encode and decode a number, say 42.

**Encryption:** c≡4217mod  3233c \equiv 42^{17} \mod 3233c≡4217mod3233

Using a calculator or program: c=2557c = 2557c=2557

**Decryption:** m≡25572753mod  3233m \equiv 2557^{2753} \mod 3233m≡25572753mod3233

Using a calculator or program: m=42m = 42m=42

Since we get back the original number, the key pair is correct.