## 2.2 Prime-Based Asymmetric Encryption

Step-wise encryption and decryption

**Step 1: Prime Numbers Selection**

Select two prime numbers P and Q such that:

1. P and Q are between 5,000 and 10,000.
2. P is coprime to $Q-1$.
3. Q is coprime to $P-1$.

Let:

- $P=7{,}091$
- $Q=8{,}317$

**Verification of coprime conditions:**

- $\gcd(P,Q-1)=\gcd(7{,}091,8{,}316)=1$.
- $\gcd(Q,P-1)=\gcd(8{,}317,7{,}090)=1$.

Hence, P and Q satisfy all conditions.

**Step 2: Compute N**

- $N=P\cdot Q=7{,}091\cdot 8{,}317=58{,}975{,}847$

**Step 3: Find P′ and Q′**

We need:

1. $P\cdot P'\equiv 1 \pmod{Q-1}$
2. $Q\cdot Q'\equiv 1 \pmod{P-1}$

Using a modular inverse calculator:

- $P'=6{,}641$ (modular inverse of 7,091 modulo 8,316).
- $Q'=3{,}249$ (modular inverse of 8,317 modulo 7,090).

**Step 4: Encrypt the Message M=5,555,555**

The encryption formula is:

C = M^N (mod N)

Using **Fermat's Little Theorem**, since M<N:

M^N (mod N) = M (mod N)

Thus:

C=5,555,555 (mod 58,975,847)=5,555,555

**Step 5: Decrypt C=5,555,555**

The decryption involves solving two congruences:

1. M≡C^P′ (mod Q)
2. M≡C^Q′ (mod P)

**Step 5.1: Solve M ≡ CP′ (mod Q)**

M ≡ 5,555,555 ^ 6,641(mod 8,317)

Using a modular exponentiation calculator:

M ≡ 5,555,555 (mod 8,317) = 3,293

**Step 5.2: Solve M≡C^Q′ (mod P):**

M≡5,555,555^3,249 (mod 7,091)

Using a modular exponentiation calculator:

- M≡5,555,555 (mod 7,091)=5,269

**Step 6: Combine Using the Chinese Remainder Theorem (CRT)**

We now solve the system of congruences:

1. M≡3,293 (mod 8,317)
2. M≡5,269 (mod 7,091)

Using the CRT solver:

M=5,555,555

Both encryption and decryption return $M=5,555,555$. Below are the detailed steps:

1. Selected primes:
   - $P=7,091$, $Q=8,317$
2. $N=58,975,847$
3. Modular inverses:
   - $P'=6,641$, $Q'=3,249$
4. Encryption:
   - $C=5,555,555$
5. Decryption:
   - $M=5,555,555$ verified via CRT.