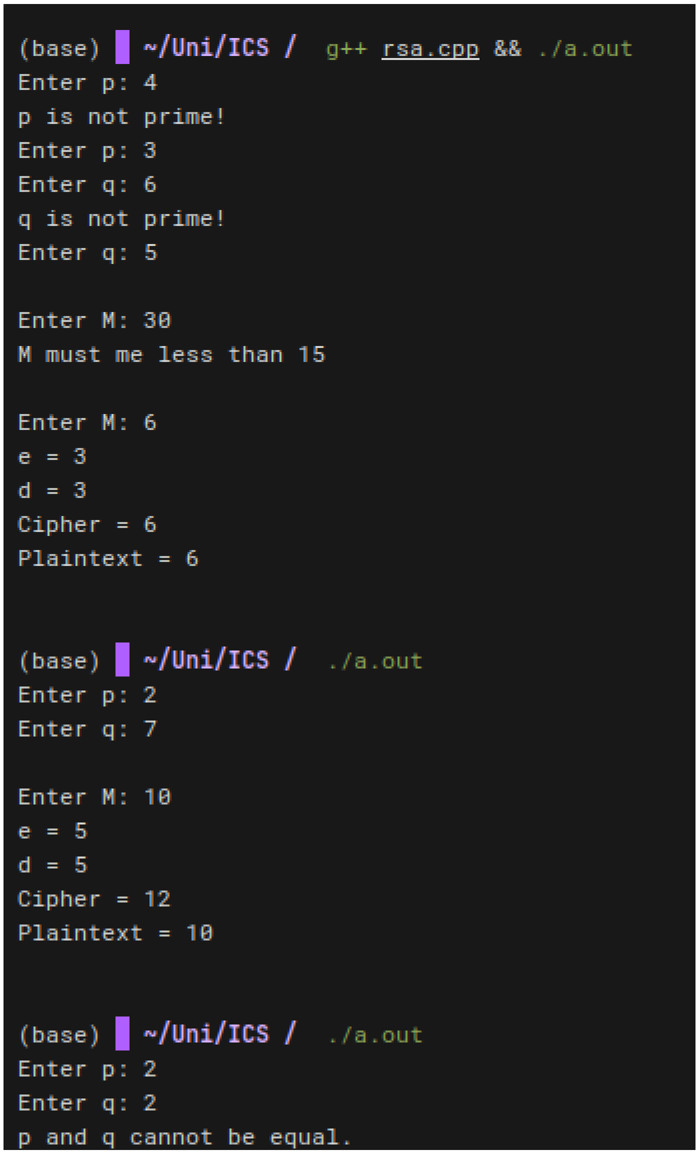
Name: Shabbar Adamjee
Roll No.: PB57
PRN: 1032221508

RSA

Code

```
#include <cmath>
#include <iostream>
#include <math.h>
#include <numeric>

bool isPrime(int num) {
  for (int i = 2; i < num; i++)
    if (num % i == 0)
      return false;

  return true;
}

int main() {
  int p, q, M;
  bool equal = false;

  do {
    equal = false;
    do {
      std::cout << "Enter p: ";
      std::cin >> p;

      if (!isPrime(p))
        std::cerr << "p is not prime!\n";
    } while (!isPrime(p));

    do {
      std::cout << "Enter q: ";
      std::cin >> q;

      if (!isPrime(q))
        std::cerr << "p is not prime!\n";

    } while (!isPrime(q));

    if (q == p) {
      std::cerr << "p and q cannot be equal.\n";
      equal = true;
    }
  } while (equal);

  int n = p * q;

  do {
    std::cout << "\nEnter M: ";
    std::cin >> M;

    if (M >= n)
      std::cerr << "M must me less than " << n << '\n';
  } while (M >= n);

  int totient = (p - 1) * (q - 1);

  int e;
  for (e = 2; e < totient; e++) {
    if (std::gcd(totient, e) == 1)
      break;
  }

  int k;
  double d;
  for (k = 0; k < e; k++) {
    d = (1 + k * totient) / double(e);

    if (d - int(d) == 0)
      break;
  }

  std::cout << "e = " << e << "\nd = " << d << std::endl;

  int cipher = int(pow(M, e)) % n;
  int plain = int(pow(cipher, d)) % n;

  std::cout << "Cipher = " << cipher << "\nPlaintext = " << plain << std::endl;

  std::cout << std::endl;
  return 0;
}
```

Output



```
(base)  ~/Uni/ICS /  g++ rsa.cpp && ./a.out
Enter p: 4
p is not prime!
Enter p: 3
Enter q: 6
q is not prime!
Enter q: 5

Enter M: 30
M must me less than 15

Enter M: 6
e = 3
d = 3
Cipher = 6
Plaintext = 6


(base)  ~/Uni/ICS /  ./a.out
Enter p: 2
Enter q: 7

Enter M: 10
e = 5
d = 5
Cipher = 12
Plaintext = 10


(base)  ~/Uni/ICS /  ./a.out
Enter p: 2
Enter q: 2
p and q cannot be equal.
```