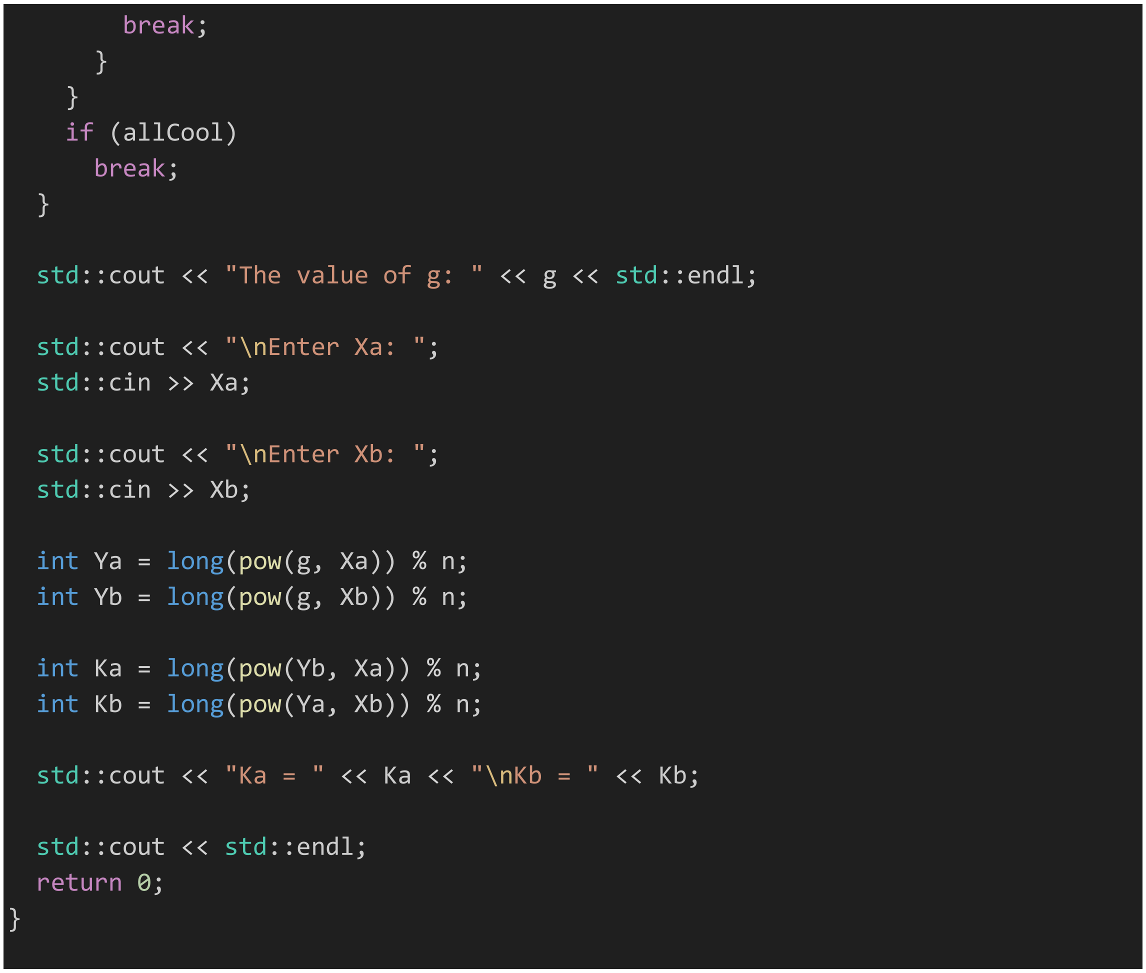
Nam : Shabbar Adamjee
Roll No.: PB57
PRN: 1032221508

ICS LAB ASSIGNMENT 6

DIFFIE HELLMAN ALGORITHM

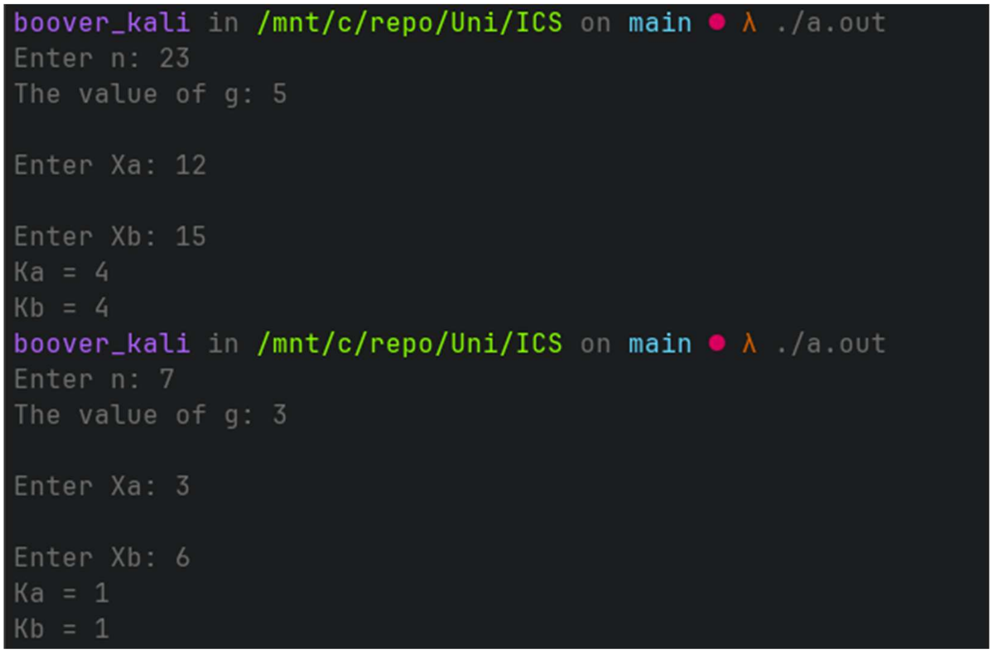
Code

```
#include <cmath>
#include <iostream>
#include <set>

bool checkG(int g, std::set<int> &valOfG) {
  const bool isIn = valOfG.find(g) != valOfG.end();

  if (!isIn) {
    valOfG.insert(g);
    return true;
  } else {
    return false;
  }
}

int main() {
  int n, Xa, Xb;
  std::set<int> valOfG;

  std::cout << "Enter n: ";
  std::cin >> n;

  int g = 2;
  bool allCool = true;

  for (; g < n; g++) {
    allCool = true;
    valOfG.clear();

    for (int i = 1; i < n; i++) {
      int val = long(pow(g, i)) % n;
      if (!checkG(val, valOfG)) {
        allCool = false;
```



```
        break;
      }
    }
    if (allCool)
      break;
  }

  std::cout << "The value of g: " << g << std::endl;

  std::cout << "\nEnter Xa: ";
  std::cin >> Xa;

  std::cout << "\nEnter Xb: ";
  std::cin >> Xb;

  int Ya = long(pow(g, Xa)) % n;
  int Yb = long(pow(g, Xb)) % n;

  int Ka = long(pow(Yb, Xa)) % n;
  int Kb = long(pow(Ya, Xb)) % n;

  std::cout << "Ka = " << Ka << "\nKb = " << Kb;

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

Output



```
boover_kali in /mnt/c/repo/Uni/ICS on main ● λ ./a.out
Enter n: 23
The value of g: 5

Enter Xa: 12

Enter Xb: 15
Ka = 4
Kb = 4
boover_kali in /mnt/c/repo/Uni/ICS on main ● λ ./a.out
Enter n: 7
The value of g: 3

Enter Xa: 3

Enter Xb: 6
Ka = 1
Kb = 1
```