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

FEISTEL CIPHER

Code

```cpp
#include <bitset>
#include <iostream>
#include <ostream>
#include <sstream>
#include <string>
#include <vector>

std::string encypt(std::string plainText, std::string key1, std::string key2) {
  std::stringstream ss(plainText);
  std::string left, right;
  ss >> left >> right;

  std::bitset<8> left_0(left);
  std::bitset<8> right_0(right);
  std::bitset<8> k1(key1);
  std::bitset<8> k2(key2);

  std::vector<std::bitset<8>> v{k1, k2};

  std::bitset<8> prev_left = left_0;
  std::bitset<8> prev_right = right_0;

  for (int i = 0; i < 2; i++) {
    std::bitset<8> next_left = prev_right;
    std::bitset<8> next_right = prev_left ^ (prev_right ^ v[i]);

    prev_left = next_left;
    prev_right = next_right;
  }

  std::string result = prev_right.to_string() + " " + prev_left.to_string();

  return result;
}

std::string decrypt(std::string cipherText, std::string key1,
                    std::string key2) {
```

```
38   std::stringstream ss(cipherText);
39   std::string left, right;
40   ss >> left >> right;
41
42   std::bitset<8> left_0(left);
43   std::bitset<8> right_0(right);
44   std::bitset<8> k1(key1);
45   std::bitset<8> k2(key2);
46
47   std::vector<std::bitset<8>> v{k2, k1};
48
49   std::bitset<8> prev_left = left_0;
50   std::bitset<8> prev_right = right_0;
51
52   for (int i = 0; i < 2; i++) {
53     std::bitset<8> next_left = prev_right;
54     std::bitset<8> next_right = prev_left ^ (prev_right ^ v[i]);
55
56     prev_left = next_left;
57     prev_right = next_right;
58   }
59
60   std::string result = prev_right.to_string() + " " + prev_left.to_string();
61
62   return result;
63 }
64
65 void displayMenu() {
66
67   char op;
68
69   do {
70     std::cout << "FESITEL CIPHER\n\n";
71     std::cout
72         << "Select an option:\n1. Encryption\n2. Decyption\n3. Exit\n\n>> ";
73     std::cin >> op;
74     std::cin.ignore();
75
76     switch (op) {
77     case '1': {
78       std::string plainText{"01001111 01001011"};
79       std::cout << "Enter plain text (space-separated): ";
80       std::getline(std::cin, plainText);
81
82       std::string key1{}, key2{};
83       std::cout << "Enter keys:\nk1: ";
```

```
84      std::cin >> key1;
85      std::cout << "k2: ";
86      std::cin >> key2;
87
88      std::cout << "The cipher is: " << encypt(plainText, key1, key2)
89                << std::endl
90                << std::endl;
91      break;
92    }
93    case '2': {
94      std::string cipherText{"01001111 01001011"};
95      std::cout << "Enter cipher text (space-separated): ";
96      std::getline(std::cin, cipherText);
97
98      std::string key1{}, key2{};
99      std::cout << "Enter keys:\nk1: ";
100      std::cin >> key1;
101      std::cout << "k2: ";
102      std::cin >> key2;
103
104      std::cout << "The plain text is: " << decrypt(cipherText, key1, key2)
105                << std::endl
106                << std::endl;
107      break;
108    }
109    case '3': {
110      std::cout << "Bye, lad\n\n";
111      break;
112    }
113    default: {
114      std::cerr << "Please select a valid option.\n\n";
115    }
116    }
117  } while (op != '3');
118 }
119
120 int main() {
121   displayMenu();
122
123   std::cout << std::endl;
124   return 0;
125 }
```

Output

```
~/Uni/ICS /  g++ feistel.cpp -g && ./a.out
FESITEL CIPHER

Select an option:
1. Encryption
2. Decyption
3. Exit

>> 1
Enter plain text (space-separated): 01001111 01001011
Enter keys:
k1: 10100110
k2: 10110111
The cipher is: 01011110 10100010

FESITEL CIPHER

Select an option:
1. Encryption
2. Decyption
3. Exit

>> 2
Enter cipher text (space-separated): 01011110 1010001
Enter keys:
k1: 10100110
k2: 10110111
The plain text is: 01001111 01001011

FESITEL CIPHER

Select an option:
1. Encryption
2. Decyption
3. Exit

>> 3
Bye, lad
```