Министерство образования Республики Беларусь

Учреждение образования

«Брестский Государственный технический университет»

Кафедра ИИТ

**Лабораторная работа №6**

По дисциплине «Криптографические методы защиты информации»

Тема: «Контроль целостности (биты четности, CRC и ECC)»

**Выполнил:**

Студент 2 курса

Группы ИИ-21

Карагодин Д. Л.

**Проверил:**

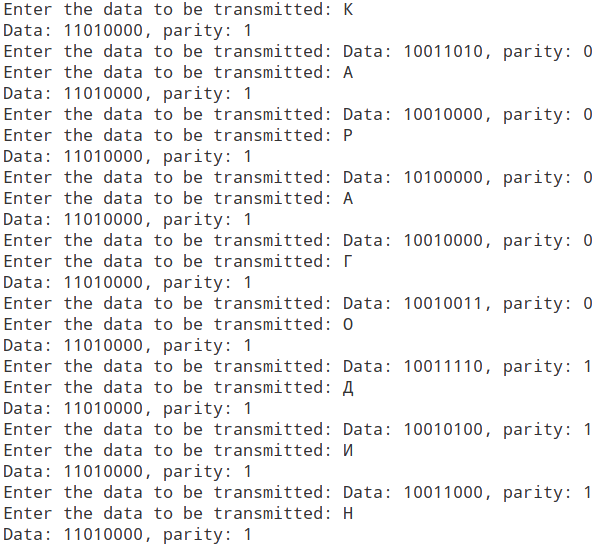
Хацкевич М. В.

Брест 2023

**Цель:** научиться проводить контроль целостности данных.

**Ход работы:**

**Биты четности**:



#include <iostream>

#include <bitset>

using namespace std;

bool parity\_bit(bitset<8> &bits){

bool parity = 0;

for(int i=0; i<8; i++)

parity ^= bits[i];

return parity;

}

int main(){

char data;

while (true){

cout << "Enter the data to be transmitted: ";

cin >> data;

bitset<8> bits(data);

cout << "Data: " << bits << ", parity: " << parity\_bit(bits) << endl;

}

}

**CRC:**

К – 1100 1010 G(x) = x4 + x1 + x0. -> 10011

А – 1100 0000

|  |  |  |  |
| --- | --- | --- | --- |
| Делимое P(x) (входные данные) | 1100 1010 | 1100 1000 | 1101 0000 |
| P(x) \* xN | 1100 1010 0000 | 1100 0000 0000 | 1101 0000 0000 |
| Деление P(x) \* xN mod G(x) |  |  |  |
| Частное | 11011100 | 11010111 | 11000100 |
| Остаток R(x) (контрольная сумма) | 0100 | 1001 | 1100 |

Р – 1101 0000

Для проверки правильности передачи рассчитаем контрольную сумму для входных данных и сравним ее с переданной суммой.

**ECC:**

К + А = 11001010111

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Номер позиции бита | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
| Обозначение бита | r1 | r2 | x1 | r3 | x2 | x3 | x4 | r4 | x5 | x6 | x7 | x8 | x9 | x10 | x11 |
| Значение бита, ХR | 0 | 0 | 1 | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 1 | 0 | 1 | 1 | 1 |
| Двоичное представление  номера позиции бита, N | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | r1 | 0 |
| 0 | 1 | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 1 | r2 | 0 |
| 0 | 0 | 0 | 1 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | r3 | 0 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | r4 | 1 |

Проверка целостности:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Номер позиции бита | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
| Обозначение бита | r1 | r2 | x1 | r3 | x2 | x3 | x4 | r4 | x5 | x6 | x7 | x8 | x9 | x10 | x11 |
| Значение бита, ХR’ | 0 | 0 | 1 | 0 | 1 | 0 | 0 | 1 | 1 | 0 | 1 | 0 | 1 | 1 | 1 | pb | 0 |
| Двоичное представление  номера позиции бита, N | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | s1 | 0 |
| 0 | 1 | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 1 | s2 | 0 |
| 0 | 0 | 0 | 1 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | s3 | 0 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | s4 | 0 |

Ошибок нет. Вектор синдромов состоит из нулей и паритетный бит равен 0.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Номер позиции бита | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
| Обозначение бита | r1 | r2 | x1 | r3 | x2 | x3 | x4 | r4 | x5 | x6 | x7 | x8 | x9 | x10 | x11 |
| Значение бита, ХR’ | 0 | 0 | 1 | 0 | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 0 | 1 | 1 | 1 | pb | 1 |
| Двоичное представление  номера позиции бита, N | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | s1 | 1 |
| 0 | 1 | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 1 | s2 | 1 |
| 0 | 0 | 0 | 1 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | s3 | 0 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | s4 | 1 |

В последовательности одиночная исправимая ошибка. Для ее исправления находим бит под номером 10112, то есть, 1110 и инвертируем его.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Номер позиции бита | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
| Обозначение бита | r1 | r2 | x1 | r3 | x2 | x3 | x4 | r4 | x5 | x6 | x7 | x8 | x9 | x10 | x11 |
| Значение бита, ХR’ | 0 | 0 | 1 | 0 | 1 | 0 | 1 | 1 | 1 | 0 | 0 | 0 | 1 | 1 | 1 | pb | 0 |
| Двоичное представление  номера позиции бита, N | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | s1 | 1 |
| 0 | 1 | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 1 | s2 | 1 |
| 0 | 0 | 0 | 1 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | s3 | 0 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | s4 | 0 |

В последовательности двоичная неисправимая ошибка.

**Вывод:** в ходе лабораторной работы научился проводить контроль целостности данных с помощью битов четности, CRC, ECC.