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-23

Романюк А. П.

Проверил:

Хацкевич А. С.

Брест 2024

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

**Ход работы:**

**CRC:**

|  |  |  |  |
| --- | --- | --- | --- |
| Буква | Битовая строка | Паритетный бит | |
| четный (odd) | нечетный (even) |
| А | 11000000 | 1 | 0 |
| Л | 11001011 | 0 | 1 |
| Е | 11000101 | 1 | 0 |

|  |  |  |  |
| --- | --- | --- | --- |
| Делимое P(x) (входные данные) | 11000000 | 11001011 | 11000101 |
| P(x) \* xN | 11000000 0000 | 11001011 0000 | 11000101 0000 |
| Деление P(x) \* xN mod G(x) | 110000000000 10011        1  10110  10011       1   01010   00000      0    10100    10011     1     01110     00000    0      11100  10011 1  11110  10011 1  11010  10011 1  1001 | 110010110000 10011        1  10100  10011       1   01111   00000      0    11111    10011     1     11000     10011    1      10110  10011 1  01010  00000 0  10100  10011 1  0111 | 110001010000 10011        1  10111  10011       1   01000   00000      0    10001    10011     1     00100     00000    0      01000  00000 0  10000  10011 1  00110  00000 0  0110 |
| Частное | 11010111 | 11011101 | 11010010 |
| Остаток R(x) (контрольная сумма) | 1001 | 0111 | 0110 |
| Входные данные с контрольной суммой | 11010111 1001 | 11011101 0111 | 11010010 0110 |

**ECC:**

Р+О = 11010000110

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 0 |
| 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 | 1 |
| 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 | 0 |

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 | 1 | 1 | 0 | 1 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 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 | 1 | 1 | 0 | 1 | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 1 | 1 | 0 | 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 | 1 | 1 | 0 | 1 | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 1 | 1 | 0 | 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.