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

Кирлович А. А.

Проверил:

Хацкевич М. В.

Брест 2023

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

**Ход работы:**

**CRC:**

|  |  |  |  |
| --- | --- | --- | --- |
| Буква | Битовая строка | Паритетный бит | |
| четный (odd) | нечетный (even) |
| К | 11001010 | 1 | 0 |
| И | 11001000 | 0 | 1 |
| Р | 11010000 | 1 | 0 |

|  |  |  |  |
| --- | --- | --- | --- |
| Делимое P(x) (входные данные) | 11001010 | 11001000 | 11010000 |
| P(x) \* xN | 110010100000 | 110010000000 | 110100000000 |
| Деление P(x) \* xN mod G(x) | 110010100000 10011         1  10100  10011        1   01111   00000       0    11110    10011      1     11010     10011     1      10010  10011 1  00010  00000 0  00100  00000 0  0100 | 110010000000 10011         1  10100  10011        1   01110   00000       0    11100    10011      1     11110     10011     1      11010  10011 1  10010  10011 1  00010  00000 0  0010 | 110100000000 10011         1  10010  10011        1   00010   00000       0    00100    00000      0     01000     00000     0      10000  10011 1  00110  00000 0  01100  00000 0  1100 |
| Частное | 11011100 | 11011110 | 11000100 |
| Остаток R(x) (контрольная сумма) | 0100 | 0010 | 1100 |
| Входные данные с контрольной суммой | 110111000100 | 110111100010 | 110001001100 |

**ECC:**

А + Р = 11000000110

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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 | 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 | 1 |
| 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 | 1 |
| 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’ | 1 | 0 | 1 | 1 | 1 | 0 | 0 | 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’ | 1 | 0 | 1 | 1 | 1 | 0 | 0 | 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’ | 1 | 0 | 1 | 1 | 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.