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

Макаревич Н.Р.

Проверил:

Хацкевич А. С.

Брест 2024

В лабораторной работе необходимо определить контрольные данные с использованием следующих способов:

- шифруемое сообщение в символьном и битовом представлении в соответствии с кодировкой Windows 1251

- синхропосылку в битовом представлении;

- результат сложения по модулю 2 шифруемого сообщения и синхропосылки;

- ключ (7 букв фамилии) в символьном и битовом представлении в соответствии с кодировкой Windows 1251;

- ключ в битовом представлении с учетом битов контроля четности;

- ключевые элементы k_i;

- битов четности. В качестве исходных данных принять битовое представление букв фамилии в соответствии с кодировкой Windows 1251

- контрольных сумм (CRC). В качестве исходных данных принять коды 1-ой, 2-ой и 3-ей буквы своей фамилии согласно их положению в алфавите; порождающего полинома - $G(x) = x^4 + x^1 + x^0$.

- кода коррекции ошибок (ECC). В качестве исходных данных принять первые 11 битов первых двух буквы своей фамилии в соответствии с кодировкой Windows 1251 Рассчитать вектор контрольных битов и вектора синдромов при отсутствии ошибки, одиночной и двойной ошибке.

Ход работы:

Буква	Битовая строка	Паритетный бит	
		четный (odd)	нечетный (even)
М	1100 1100	1	0
А	1100 0000	1	0
К	1100 1010	1	0
А	1100 0000	1	0
Р	1101 0000	0	1
Е	1100 0101	1	0
В	1100 0010	0	1

Использование контрольных сумм

Делимое P(x) (входные данные)	1100 1100	1100 0000	1100 1010
P(x) * x^N	1100 1100 0000	1100 0000 0000	1100 1010 0000
Деление P(x) * x^N mod G(x)	110011000000 10011 1 10101 10011 1 01100 00000 0 11000 10011 1 10110 10011 1 01010 00000 0 10100 10011 1 0111	110000000000 10011 1 10110 10011 1 01010 00000 0 10100 10011 1 01110 00000 0 11100 10011 1 11110 10011 1 1101	110010100000 10011 1 10100 10011 1 01111 00000 0 11110 10011 1 11010 10011 1 10010 10011 1 00010 00000 0 0010
Частное	1101101	1101011	1101110
Остаток R(x) (контрольная сумма)	0111	1101	0010
Входные данные с контрольной суммой	110011000111	110000001101	110010100010

Использование ECC

M + A = 1100 1100 110

Номер позиции бита	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15		
Обозначение бита	r_1	r_2	x_1	r_3	x_2	x_3	x_4	r_4	x_5	x_6	x_7	x_8	x_9	x_{10}	x_{11}		
Значение бита, XR	0	0	1	0	1	0	0	0	1	1	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	r_1	0
	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1	r_2	1
	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1	r_3	1
	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	r_4	0

Проверка целостности:

Номер позиции бита	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15		
Обозначение бита	r_1	r_2	x_1	r_3	x_2	x_3	x_4	r_4	x_5	x_6	x_7	x_8	x_9	x_{10}	x_{11}		
Значение бита, XR’	1	1	1	0	1	0	0	0	1	1	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	s_1	0
	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1	s_2	0
	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1	s_3	0
	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	s_4	0

Вектор синдромов состоит из нулей, паритетный бит равен 0.

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