

7. Практическая работа. Изучение принципа работы цифрового скремблера/дескремблера

7.1. Цель работы

Изучить общие принципы работы цифрового скремблера/дескремблера. Научиться строить схемы скремблеров/дескремблеров разных типов.

7.2. Рекомендуемая литература

1. Скремблер [электронный ресурс] // Википедия : [сайт]
URL: <https://ru.wikipedia.org/wiki/Скремблер>.
2. Скремблеры [электронный ресурс] // CIT Forum : [сайт]
URL: http://citforum.ru/internet/infsecure/its2000_15.shtml

7.3. Порядок выполнения задания

Задание выполняется каждым учащимся индивидуально. По результатам выполнения работы должен быть написан отчет.

Отчёт формируется в рукописном или печатном виде.

Таблица 7.1

Варианты задания (указаны согласно номеру студента в журнале)

№ вар.	$L^{[ss]}$	$R_1^{[ss]}$	$I_{2-10}^{[inf]}$	$P_1^{[add]}$	$P_2^{[add]}$
1	13	7	92766537	$x^4 + x^2 + 1$	$x^8 + x^4 + x^3 + x^2 + 1$
2	13	11	94534225	$x^4 + x^3 + x^2 + 1$	$x^8 + x^5 + x^3 + x^1 + 1$
3	13	10	83656281	$x^4 + x^3 + x^1 + 1$	$x^8 + x^5 + x^3 + x^2 + 1$
4	13	9	84680943	$x^4 + x^2 + x^1 + 1$	$x^8 + x^6 + x^3 + x^2 + 1$
5	13	8	96802547	$x^4 + x^2 + 1$	$x^8 + x^6 + x^5 + x^1 + 1$
6	13	6	97889363	$x^4 + x^3 + x^2 + 1$	$x^8 + x^6 + x^5 + x^2 + 1$
7	13	5	86563629	$x^4 + x^3 + x^1 + 1$	$x^8 + x^6 + x^5 + x^3 + 1$
8	13	4	97553893	$x^4 + x^2 + x^1 + 1$	$x^8 + x^6 + x^5 + x^4 + 1$
9	13	3	96739033	$x^4 + x^2 + 1$	$x^9 + x^4 + x^3 + x^1 + 1$
10	13	2	94673925	$x^4 + x^3 + x^2 + 1$	$x^9 + x^5 + x^3 + x^2 + 1$
11	14	12	84673907	$x^4 + x^3 + x^1 + 1$	$x^9 + x^5 + x^4 + x^1 + 1$
12	14	11	86789093	$x^4 + x^2 + x^1 + 1$	$x^8 + x^7 + x^2 + x^1 + 1$
13	14	10	97653899	$x^4 + x^2 + 1$	$x^8 + x^7 + x^3 + x^2 + 1$
14	14	9	86764349	$x^4 + x^3 + x^2 + 1$	$x^8 + x^7 + x^5 + x^3 + 1$
15	14	8	87634295	$x^4 + x^3 + x^1 + 1$	$x^8 + x^7 + x^6 + x^1 + 1$
16	14	7	90773625	$x^4 + x^2 + x^1 + 1$	$x^9 + x^6 + x^4 + x^3 + 1$
17	14	6	86643999	$x^4 + x^2 + 1$	$x^9 + x^6 + x^5 + x^3 + 1$
18	14	5	88443773	$x^4 + x^3 + x^2 + 1$	$x^9 + x^7 + x^2 + x^1 + 1$
19	14	4	89942473	$x^4 + x^3 + x^1 + 1$	$x^9 + x^7 + x^4 + x^2 + 1$
20	14	3	98743663	$x^4 + x^2 + x^1 + 1$	$x^9 + x^7 + x^5 + x^1 + 1$
21	12	10	97274925	$x^4 + x^2 + 1$	$x^9 + x^7 + x^5 + x^2 + 1$
22	12	9	92837647	$x^4 + x^3 + x^2 + 1$	$x^9 + x^7 + x^6 + x^4 + 1$

Варианты задания (указаны согласно номеру студента в журнале)

№ вар.	$L^{[ss]}$	$R_1^{[ss]}$	$I_{2-10}^{[inf]}$	$P_1^{[add]}$	$P_2^{[add]}$
23	12	8	87662493	$x^4 + x^3 + x^1 + 1$	$x^9 + x^8 + x^4 + x^1 + 1$
24	12	7	87234227	$x^4 + x^2 + x^1 + 1$	$x^9 + x^8 + x^4 + x^2 + 1$
25	12	6	98236723	$x^4 + x^2 + 1$	$x^9 + x^8 + x^5 + x^1 + 1$
26	12	5	87236729	$x^4 + x^3 + x^2 + 1$	$x^9 + x^8 + x^5 + x^4 + 1$
27	12	4	89236243	$x^4 + x^3 + x^1 + 1$	$x^9 + x^8 + x^6 + x^5 + 1$
28	12	3	87234627	$x^4 + x^2 + x^1 + 1$	$x^9 + x^8 + x^7 + x^2 + 1$
29	11	8	95253793	$x^4 + x^2 + 1$	$x^9 + x^7 + x^2 + x^1 + 1$
30	11	7	97235463	$x^4 + x^3 + x^2 + 1$	$x^8 + x^6 + x^5 + x^3 + 1$

7.3.1. Самосинхронизирующиеся скремблеры

1. Выбрать из табл. 7.1 исходные данные для расчета.
2. Для заданных параметров (длина регистра $L^{[ss]}$ и разряды регистра $R_1^{[ss]}$ и $R_2^{[ss]} = L^{[ss]}$, охваченные обратной связью) нарисовать схемы самосинхронизирующегося скремблера и соответствующего ему дескремблера.
3. Передать через скремблер двоичную информационную комбинацию $I_{2-10}^{[inf]}$ длиной 32 разряда. Комбинация задана в табл. 7.1 в двоично-десятичном виде. Процедуру работы скремблера (состояния ячеек регистра r_i) и результат записать в виде табл. 7.2.

Таблица 7.2

Форма записи процедуры работы скремблера

Такт	IN	r_1	r_2	r_3	...	r_{L-1}	r_L	r_{out}	OUT
1					...				
2					...				
...					...				
31					...				
32					...				

4. Получившийся результат передать через схему дескремблера. Процедуру работы дескремблера (состояния ячеек регистра r_i) и результат записать в виде табл. 7.2. Убедиться, что результат соответствует заданной информационной комбинации.
5. Внести одиночную ошибку в результат скремблирования и передать комбинацию с ошибкой через схему дескремблера. Процедуру работы дескремблера (состояния ячеек регистра r_i) и результат записать в виде табл. 7.2. Сравнить результат с исходной информационной комбинацией. Сделать выводы по полученным результатам.

7.3.2. Аддитивные скремблеры

1. Выбрать из табл. 7.1 исходные данные для расчета.

2. Для заданного полинома $P_1^{[add]}$ нарисовать схему аддитивного скремблера/дескремблера.

3. Проинициализировать регистр скремблера $P_1^{[add]}$ различными двоичными комбинациями и нарисовать диаграмму состояний и переходов между ними с указанием полученных циклов. Состояния и переходы между ними оформить в виде табл. 7.3 и в виде диаграммы по образцу, приведенному в лекциях.

Таблица 7.3

Форма записи состояний работы скремблера

Состояние	r_1	r_2	r_3	r_4
1				
2				
...				
15				
16				

4. Для заданного неприводимого полинома $P_2^{[add]}$ построить схему аддитивного скремблера/дескремблера.

5. Передать через скремблер информационную комбинацию $I_{2-10}^{[inf]}$ длиной 32 разряда. Комбинация задана в табл. 7.1 в двоично-десятичном виде. Процедуру работы скремблера и результат записать в виде табл. 7.2.

6. Получившийся результат передать через схему дескремблера. Процедуру работы дескремблера и результат записать в виде табл. 7.2. Убедиться, что результат соответствует заданной информационной комбинации.

7. Внести одиночную ошибку в результат скремблирования и передать комбинацию с ошибкой через схему дескремблера. Процедуру работы дескремблера и результат записать в виде табл. 7.2. Сравнить результат с исходной информационной комбинацией. Сделать выводы по полученным результатам.

7.4. Порядок защиты практической работы

Защита работы может осуществляться одним из нижеперечисленных способов или их сочетанием на усмотрение преподавателя.

1. Устный ответ по теме работы.
2. Тестирование по теме работы
3. Задача по теме работы.
4. Иные варианты на усмотрение преподавателя.