# ЗАДАНИЕ 1

Проверить свойства сбалансированности, корреляционной иммунности, лавинного критерия и нелинейности для булевой функции от 4 переменных: x4⊕x3⊕x2x3⊕x1⊕x1x3x4⊕x1x2x4

## СБАЛАНСИРОВАННОСТЬ

Свойство сбалансированности говорит о том, что количество нулей и единиц в таблице истинности булевой функции должно примерно совпадать.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| x1 | x2 | x3 | x4 | x4⊕x3⊕x2x3⊕x1⊕x1x3x4⊕x1x2x4 |
| 0 | 0 | 0 | 0 | 0 |
| 0 | 0 | 0 | 1 | 1 |
| 0 | 0 | 1 | 0 | 1 |
| 0 | 0 | 1 | 1 | 0 |
| 0 | 1 | 0 | 0 | 0 |
| 0 | 1 | 0 | 1 | 1 |
| 0 | 1 | 1 | 0 | 0 |
| 0 | 1 | 1 | 1 | 1 |
| 1 | 0 | 0 | 0 | 1 |
| 1 | 0 | 0 | 1 | 0 |
| 1 | 0 | 1 | 0 | 0 |
| 1 | 0 | 1 | 1 | 0 |
| 1 | 1 | 0 | 0 | 1 |
| 1 | 1 | 0 | 1 | 1 |
| 1 | 1 | 1 | 0 | 1 |
| 1 | 1 | 1 | 1 | 0 |

В данном случае количество нулей и единиц равно 8. Значит свойство сбалансированности выполняется.

## КОРРЕЛЯЦИОННАЯ ИММУННОСТЬ

Свойство корреляционной иммунности говорит о том, что при замене одной из переменных на константу функция должна измениться.

| x1 | x2 | x3 | x4 |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 1 |
| 0 | 0 | 0 | 1 | 1 | 1 | 0 | 1 | 1 | 1 | 0 | 0 | 1 |
| 0 | 0 | 1 | 0 | 1 | 1 | 0 | 1 | 0 | 0 | 1 | 1 | 0 |
| 0 | 0 | 1 | 1 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 1 | 0 |
| 0 | 1 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 1 |
| 0 | 1 | 0 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 0 | 1 |
| 0 | 1 | 1 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 0 | 0 | 1 |
| 0 | 1 | 1 | 1 | 1 | 1 | 0 | 0 | 1 | 1 | 1 | 0 | 1 |
| 1 | 0 | 0 | 0 | 1 | 0 | 1 | 1 | 1 | 1 | 0 | 1 | 0 |
| 1 | 0 | 0 | 1 | 0 | 1 | 0 | 0 | 1 | 0 | 0 | 1 | 0 |
| 1 | 0 | 1 | 0 | 0 | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 0 |
| 1 | 0 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 1 | 0 | 0 | 1 | 0 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| 1 | 1 | 0 | 1 | 1 | 1 | 1 | 0 | 1 | 1 | 0 | 1 | 1 |
| 1 | 1 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 1 | 1 | 1 | 0 |
| 1 | 1 | 1 | 1 | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 1 | 0 |
| Количество различий | | | | | 6 | 6 | 4 | 4 | 4 | 4 | 6 | 6 |

Количество изменившихся значений составляет 50%-75%. В идеале он должен быть 50%. В целом можно считать критерий корреляционной иммунности выполненным.

## НЕЛИНЕЙНОСТЬ

Свойство нелинейности говорит о том, что функцию нельзя преобразовать в линейную. Для того, чтобы проверить это свойство, сравним таблицы истинности всех линейных функций от 4 элементов с таблицей истинности нашей функции.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | x1 | x2 | x3 | x4 |  |  |  |  |  |  |  |  |  |  |  |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 0 | 0 | 1 | 0 | 0 | 1 | 0 | 1 | 1 | 0 | 1 | 1 | 1 | 1 |
| 1 | 0 | 0 | 1 | 0 | 0 | 1 | 0 | 1 | 0 | 1 | 1 | 0 | 1 | 1 | 1 |
| 0 | 0 | 0 | 1 | 1 | 0 | 1 | 1 | 1 | 1 | 0 | 1 | 1 | 0 | 0 | 0 |
| 0 | 0 | 1 | 0 | 0 | 1 | 0 | 0 | 1 | 1 | 0 | 1 | 1 | 0 | 1 | 1 |
| 1 | 0 | 1 | 0 | 1 | 1 | 0 | 1 | 1 | 0 | 1 | 1 | 0 | 1 | 0 | 0 |
| 0 | 0 | 1 | 1 | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 0 | 1 | 1 | 0 | 0 |
| 1 | 0 | 1 | 1 | 1 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 |
| 1 | 1 | 0 | 0 | 0 | 1 | 1 | 1 | 0 | 0 | 0 | 1 | 1 | 1 | 0 | 1 |
| 0 | 1 | 0 | 0 | 1 | 1 | 1 | 0 | 0 | 1 | 1 | 1 | 0 | 0 | 1 | 0 |
| 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 |
| 0 | 1 | 0 | 1 | 1 | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 0 | 1 | 0 | 1 |
| 1 | 1 | 1 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 0 | 0 | 0 | 1 | 1 | 0 |
| 1 | 1 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 0 | 1 |
| 1 | 1 | 1 | 1 | 0 | 0 | 0 | 1 | 0 | 1 | 1 | 1 | 0 | 0 | 0 | 1 |
| 0 | 1 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 0 |
| Различия | 8 | 6 | 10 | 8 | 10 | 6 | 4 | 8 | 10 | 6 | 8 | 10 | 6 | 8 | 4 |

Степень нелинейности равна минимальному количеству различий функции с какой-либо линейной функцией. В данном случае она равна 4.

## ЛАВИННЫЙ КРИТЕРИЙ

*Производной* булевой функции по направлению называют

Булева функция удовлетворяет *лавинному критерию*, если

| x1 | x2 | x3 | x4 |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 0 | 0 | 0 | 1 | 0 | 1 | 1 |
| 0 | 0 | 0 | 1 | 1 | 0 | 1 | 1 |
| 0 | 0 | 1 | 0 | 1 | 1 | 1 | 1 |
| 0 | 0 | 1 | 1 | 0 | 1 | 1 | 1 |
| 0 | 1 | 0 | 0 | 1 | 0 | 0 | 1 |
| 0 | 1 | 0 | 1 | 0 | 0 | 0 | 1 |
| 0 | 1 | 1 | 0 | 1 | 1 | 0 | 1 |
| 0 | 1 | 1 | 1 | 1 | 1 | 0 | 1 |
| 1 | 0 | 0 | 0 | 1 | 0 | 1 | 1 |
| 1 | 0 | 0 | 1 | 1 | 1 | 0 | 1 |
| 1 | 0 | 1 | 0 | 1 | 1 | 1 | 0 |
| 1 | 0 | 1 | 1 | 0 | 0 | 0 | 0 |
| 1 | 1 | 0 | 0 | 1 | 0 | 0 | 0 |
| 1 | 1 | 0 | 1 | 0 | 1 | 1 | 0 |
| 1 | 1 | 1 | 0 | 1 | 1 | 0 | 1 |
| 1 | 1 | 1 | 1 | 1 | 0 | 1 | 1 |
|  | | | | 12 | 8 | 8 | 12 |

Для и условия лавинного критерия нарушаются.

Лавинный критерий не выполняется.

# ЗАДАНИЕ 2

Выполнить шифрование методом перестановки в колонках.

|  |  |
| --- | --- |
| ключ | Текст |
| 1,7,2,8,3,5,4,9,6 | Схема предварительного распределения ключей состоит из двух алгоритмов: распределения исходной ключевой информации и формирования ключа. |

Уберём из исходного текста все знаки пунктуации. Приведём все буквы к верхнему регистру.

СХЕМАПРЕДВАРИТЕЛЬНОГОРАСПРЕДЕЛЕНИЯКЛЮЧЕЙСОСТОИТИЗДВУХАЛГОРИТМОВРАСПРЕДЕЛЕНИЯИСХОДНОЙКЛЮЧЕВОЙИНФОРМАЦИИИФОРМИРОВАНИЯКЛЮЧА.

Так как длина ключа 9, то разобьем исходный текст на 9 колонок.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| С | Х | Е | М | А | П | Р | Е | Д |
| В | А | Р | И | Т | Е | Л | Ь | Н |
| О | Г | О | Р | А | С | П | Р | Е |
| Д | Е | Л | Е | Н | И | Я | К | Л |
| Ю | Ч | Е | Й | С | О | С | Т | О |
| И | Т | И | З | Д | В | У | Х | А |
| Л | Г | О | Р | И | Т | М | О | В |
| Р | А | С | П | Р | Е | Д | Е | Л |
| Е | Н | И | Я | И | С | Х | О | Д |
| Н | О | Й | К | Л | Ю | Ч | Е | В |
| О | Й | И | Н | Ф | О | Р | М | А |
| Ц | И | И | И | Ф | О | Р | М | И |
| Р | О | В | А | Н | И | Я | К | Л |
| Ю | Ч | А |  |  |  |  |  |  |

Переставим колонки согласно ключу.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| С | Р | Х | Е | Е | А | М | Д | П |
| В | Л | А | Ь | Р | Т | И | Н | Е |
| О | П | Г | Р | О | А | Р | Е | С |
| Д | Я | Е | К | Л | Н | Е | Л | И |
| Ю | С | Ч | Т | Е | С | Й | О | О |
| И | У | Т | Х | И | Д | З | А | В |
| Л | М | Г | О | О | И | Р | В | Т |
| Р | Д | А | Е | С | Р | П | Л | Е |
| Е | Х | Н | О | И | И | Я | Д | С |
| Н | Ч | О | Е | Й | Л | К | В | Ю |
| О | Р | Й | М | И | Ф | Н | А | О |
| Ц | Р | И | М | И | Ф | И | И | О |
| Р | Я | О | К | В | Н | А | Л | И |
| Ю |  | Ч |  | А |  |  |  |  |

Соберём полученную комбинацию обратно в текст.

СРХЕЕАМДПВЛАЬРТИНЕОПГРОАРЕСДЯЕКЛНЕЛИЮСЧТЕСЙООИУТХИДЗАВЛМГООИРВТРДАЕСРПЛЕЕХНОИИЯДСНЧОЕЙЛКВЮОРЙМИФНАОЦРИМИФИИОРЯОКВНАЛИЮ\_Ч\_А\_\_\_\_

Чтобы усложнить криптоанализ, можно также заменить паддинги на случайные буквы.

СРХЕЕАМДПВЛАЬРТИНЕОПГРОАРЕСДЯЕКЛНЕЛИЮСЧТЕСЙООИУТХИДЗАВЛМГООИРВТРДАЕСРПЛЕЕХНОИИЯДСНЧОЕЙЛКВЮОРЙМИФНАОЦРИМИФИИОРЯОКВНАЛИЮАЧБАВГДЕ

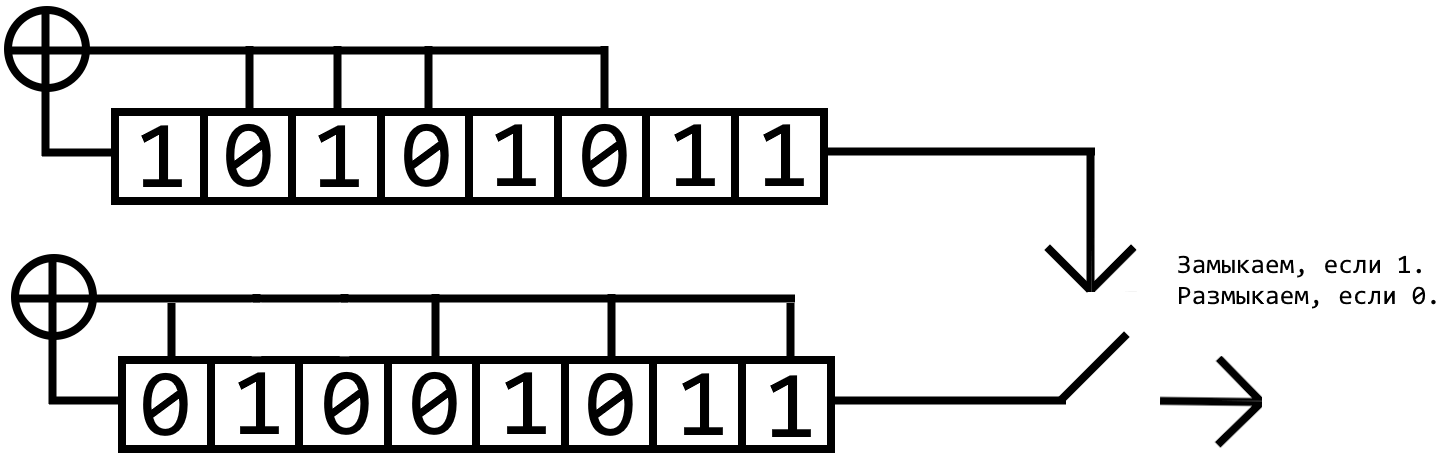
# ЗАДАНИЕ 3

Получить 16 знаков гаммы для следующих типов генераторов.

|  |  |  |
| --- | --- | --- |
| Схема | Холостой ход | Начальное состояние |
| Сжимающий генератор:  PCОЛС1 n = 8, x1+x2+x3+x5  РСОЛС2 n = 8, x0+x3+x5+x7 | 15 | 1010101101001011 |

При выполнении задания необходимо нарисовать схему и расписать подробно первые и последние 3 такта (всего 6 тактов) работы генератора.

Схема:



Такты первого РСОЛС:

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| 1 | 0 | 1 | 0 | 1 | 0 | 1 | 1 |

| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | 1 | 0 | 1 | 0 | 1 | 0 | 1 |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| 1 | 1 | 1 | 0 | 1 | 0 | 1 | 0 |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| 0 | 1 | 1 | 1 | 0 | 1 | 0 | 1 |

…

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| 1 | 0 | 1 | 1 | 1 | 0 | 0 | 0 |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| 0 | 1 | 0 | 1 | 1 | 1 | 0 | 0 |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| 1 | 0 | 1 | 0 | 1 | 1 | 1 | 0 |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| 0 | 1 | 0 | 1 | 0 | 1 | 1 | 1 |

Такты второго РСОЛС:

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| 0 | 1 | 0 | 0 | 1 | 0 | 1 | 1 |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| 1 | 0 | 1 | 0 | 0 | 1 | 0 | 1 |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| 1 | 1 | 0 | 1 | 0 | 0 | 1 | 0 |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| 0 | 1 | 1 | 0 | 1 | 0 | 0 | 1 |

…

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| 0 | 1 | 0 | 0 | 1 | 0 | 0 | 0 |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| 0 | 0 | 1 | 0 | 0 | 1 | 0 | 0 |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| 1 | 0 | 0 | 1 | 0 | 0 | 1 | 0 |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| 0 | 1 | 0 | 0 | 1 | 0 | 0 | 1 |

Выработанные генераторами последовательности:

110101011100001110101011100001

000101100011011011111100100001

Полученная гамма:

0011000101110011