УДК 004.056.55

Студ. Сятковская Е. Д., Коржова В. С.

Науч. рук. Профессор П.П. Урбанович (кафедра инф. систем и технологий, БГТУ)

**АНАЛИЗ ЛАВИННОГО ЭФФЕКТА В АЛГОРИТМЕ DES**

Эффект лавины означает, что даже небольшие изменения входных данных должны привести к сильным изменениям выходных данных. Лавинный эффект является важным свойством криптографических алгоритмов, так как если алгоритм не обладает им в достаточной степени, то криптоаналитик может использовать выходные данные алгоритма для того, чтобы сделать предположения о входных данных. Поэтому разработчики криптографических алгоритмов стремятся к достижению максимального лавинного эффекта.

Цель нашей работы: изучить лавинный эффект в алгоритме DES и выяснить, как исходное сообщение и номер измененного бита влияет на проявление лавинного эффекта.

Для достижения вышепоставленных целей написана программная реализация алгоритма DES. Зашифровав сообщение длиной в 64 бита без измененного бита и с измененным битом была составлена таблица 1, демонстрирующая сравнение исходных входных последовательностей битов и зашифровки сообщений на каждом из 16 раундов Фейстеля.

**Таблица 1 – Сравнение последовательностей битов**

|  |  |  |
| --- | --- | --- |
| Раунд | **Шифротекст без измененного бита** | **Шифротекст с измененным битом** |
| - | 01100001011101100110010101100110 01100110011001010110001101110100 | 01100001011101100110110101100110  01100110011001010110001101110100 |
| 1 | 00000000111111110000000001011010 00101010100011000101001101100110 | 00000000111111110000010001011010  00111010101011000111001101100110 |
| 2 | 00101010100011000101001101100110 11011110111001001011111100111110 | 00111010101011000111001101100110  11111011011001011111100000101000 |
| 3 | 11011110111001001011111100111110 00110011011000100100001110100110 | 11111011011001011111100000101000  00011011111110010101101011000001 |
| 4 | 00110011011000100100001110100110 10111111001000010000101101010101 | 00011011111110010101101011000001  01111001100000001100010000101111 |
| 5 | 10111111001000010000101101010101 10000000111100110111000100101001 | 01111001100000001100010000101111  01000011100001011110000000101101 |
| 6 | 10000000111100110111000100101001 11011100011001011000011001111111 | 01000011100001011110000000101101  10111001000001000000001010100000 |
| 7 | 11011100011001011000011001111111 00011111000111101100101101000110 | 10111001000001000000001010100000  00101100100001001001010000010001 |
| 8 | 00011111000111101100101101000110 00100001011001011000100110010110 | 00101100100001001001010000010001  00011100101010101100010010111111 |
| 9 | 00100001011001011000100110010110 10000101100100110100100111010101 | 00011100101010101100010010111111  01000001011100100111101001011000 |
| 10 | 10000101100100110100100111010101 11000100100110100001110110001101 | 01000001011100100111101001011000  00000000100101100111000011101011 |
| 11 | 11000100100110100001110110001101 10010011001011001001110010010111 | 00000000100101100111000011101011  11001001001011110101000001001000 |
| 12 | 10010011001011001001110010010111 00010111000111101011001001100101 | 11001001001011110101000001001000  10000010110100000100000100100000 |
| 13 | 00010111000111101011001001100101 00111010101000000001110010000010 | 10000010110100000100000100100000  11010011000010010001111111011001 |
| 14 | 00111010101000000001110010000010 11000110101001101010110000111111 | 11010011000010010001111111011001  10110111011000100010110011110100 |
| 15 | 11000110101001101010110000111111 11011001100011000001110000011001 | 10110111011000100010110011110100  10011111110101101000011111011110 |
| 16 | 11011001100011000001110000011001 10111000101010000011000010110010 | 10011111110101101000011111011110  01001100000100001101011010000110 |

После прохождения всех раундов было изменено 34 бита. Посчитав по формуле , несложно сделать вывод о том, что рассматриваемый алгоритм удовлетворяет требованиям лавинного критерия, т.к. чем меньше значение лавинного параметра, тем сильнее лавинный эффект в преобразовании. Построим график зависимости количества измененных бит от номера раунда.



**Рисунок 1. — График зависимости количества измененных бит от номера раунда**

Из графика видно, что изменение половины битов происходит уже на 5 раунде.

Зашифровав 5 различных сообщений с разной длиной, была составлена таблица 2, демонстрирующая влияние исходного сообщения на лавинный эффект.

**Таблица 2 – Влияние исходного сообщения на лавинный эффект**

|  |  |  |  |
| --- | --- | --- | --- |
| Сообщение | Шифротекст | Шифротекст с измененным битом | Количество бит |
| hiworld | 1111000111001011  0000110010111110 1010011001001101  1111101111100110 | 1111011011111111  0110110000111010  0010011000111101  1001000011101100 | 21 |
| byeworld | 0011000110110000  1010010101000100 0110100110000011  0101011111010100 | 0100100101100001  1100010001011000  0111100101101111  0010000100101011 | 33 |
| desdes | 1100100101001101  0011100111111111 1000001011111111  0000001010101001 | 0011000000101100  0101011101111010  0100111101111011  1110000000111001 | 28 |
| science | 1100001111001111  0111110011100001 0001101100111100  1110111101111101 | 1111100000011001  0111010100010000  1101001000011001  0011000110011010 | 36 |
| computer | 1001100000101111  0101100101000000 1100010110010001  0010011000001001 | 0101100011010110  0000000101000111  0111010010100001  0000100101000111 | 29 |

Посчитаем процент измененных битов для каждого сообщения по формуле:

Посчитав средний процент измененных битов по формуле:

Можно сделать вывод о том, что лавинный критерий зависит от самого сообщения. Вычислив лавинный параметр, получаем что вне зависимости от сообщения рассматриваемый алгоритм удовлетворяет требованиям лавинного критерия.

Продемонстрируем влияние номера измененного бита на лавинный эффект с помощью таблицы 3.

**Таблица 3 – Влияние номера измененного бита на лавинный эффект**

|  |  |  |  |
| --- | --- | --- | --- |
| № бита | Сообщение с измененным битом | Шифротекст с измененным битом | Количество измененных битов |
| 1 | 1110000101110110  0110010101100110 0110011001100101  0110001101110100 | 0100000000100100  0110100010000110  1101001011001001  1100110110001001 | 32 |
| 64 | 0110000101110110  0110010101100110 0110011001100101  0110001101110101 | 1000111001001001  0010111001000110  0110011010000111  0101010010010111 | 31 |
| 21 | 1101100110001100  0001110000011001 1011100010101000  0011000010110010 | 1001111111010110  1000011111011110  0100110000010000  1101011010000110 | 34 |
| 45 | 0110000101110110  0110010101100110 0110011001101101  0110001101110100 | 1000011100001011  0100100100101010  1111110000011000  1100000110011011 | 36 |
| 10 | 0110000100110110  0110010101100110 0110011001100101  0110001101110100 | 0100011111100100  1111001001101010  0000100010000001  0001011001101001 | 32 |

Посчитаем разницу между максимальным значением процента измененных бит и минимальным значением по формуле:

ЛИТЕРАТУРА

1. Урбанович, П. П. Лабораторный практикум по дисциплинам «Защита информации и надежность информационных систем» и «Криптографические методы защиты информации». В 2 ч. Ч. 1. Кодирование информации: учеб.-метод. пособие для студентов учреждений высшего образования / П. П. Урбанович, Д. В. Шиман, Н. П. Шутько. – Минск: БГТУ, 2019. – 116 с. (https://elib.belstu.by/ handle/123456789/29372)
2. Vergili I., Yücel M. D. // Turk J Elec Engin. 2001. Т. 9, №. 2. С. 137-145.