МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное автономное образовательное учреждение высшего образования
«САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
АЭРОКОСМИЧЕСКОГО ПРИБОРОСТРОЕНИЯ»

КАФЕДРА № 51

ОТЧЕТ
ЗАЩИЩЕН С ОЦЕНКОЙ

ПРЕПОДАВАТЕЛЬ

ассистент		М.Н. Исаева
должность, уч. степень, звание	подпись, дата	инициалы, фамилия

ОТЧЕТ О ЛАБОРАТОРНОЙ РАБОТЕ №2

БЛОКОВЫЕ ШИФРЫ

по курсу: КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ
ЗАЩИТЫ ИНФОРМАЦИИ

РАБОТУ ВЫПОЛНИЛ

СТУДЕНТ ГР. № 5911		А.А. Бенцлер
	подпись, дата	инициалы, фамилия

Санкт-Петербург 2021

Цель работы

Реализовать алгоритм шифрования FEAL. Предусмотреть возможность работы алгоритма в режиме OFB. Исследовать процесс распространения ошибок в реализуемом режиме шифрования, привести пример распространения ошибок. Реализация каждой системы должна работать в двух режимах: шифрования и дешифрования, позволять вводить ключ вручную и генерировать его автоматически. Вычислить коэффициент корреляции для входного и выходного потока алгоритма шифрования, оценить распределение «0» и «1» в выходном потоке. По результатам анализа сделать выводы о качестве реализованной системы шифрования.

1. Алгоритм

FEAL4 это блочный шифр, с размером блока и длиной ключа равными 64 бита.
Шифр состоит из 4-х раундов и использует шесть 32-битных подключей, генерируемых из основного ключа.

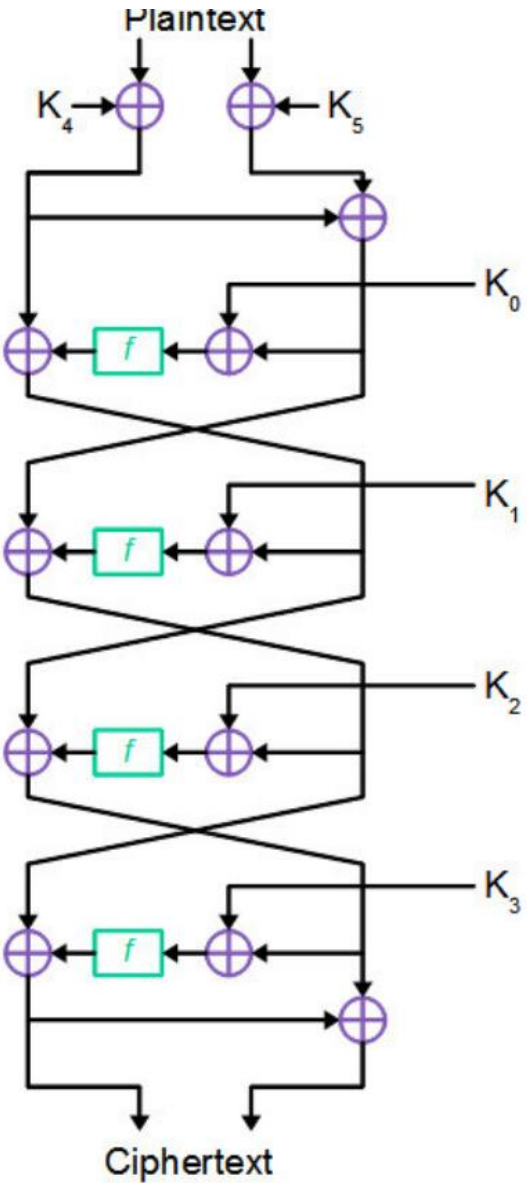

Рис.1 – алгоритм FEAL.

На начальном этапе открытый текст разбивается на два блока, по 32 бита каждый. Левый и правый блоки складываются по модулю два с 32-битными подключами K[4] и K[5] соответственно. Затем левая часть остается без изменений, а правая образуется сложением по модулю два с левым блоком.

После этого выполняется 4 раунда шифрования на каждом из которых правый блок суммируется по модулю два с подключом раунда K[i], а затем полученный результат прогоняется через функцию перестановки F. Результат перестановки складывается с левой частью текста. После этих операций левый и правый блок меняют местами и полученный результат подается на вход следующего раунда.

Последний раунд немного отличается от всех остальных. Левые и правые блоки не меняются местами, как в предыдущих раундах.
Вместо этого, правый блок складывается по модулю два с левым блоком и полученный результат возвращается в качестве правой части шифротекста. Левая же часть после 4 раунда остается неизменной и составляет первые 32 бита полученного шифротекста.

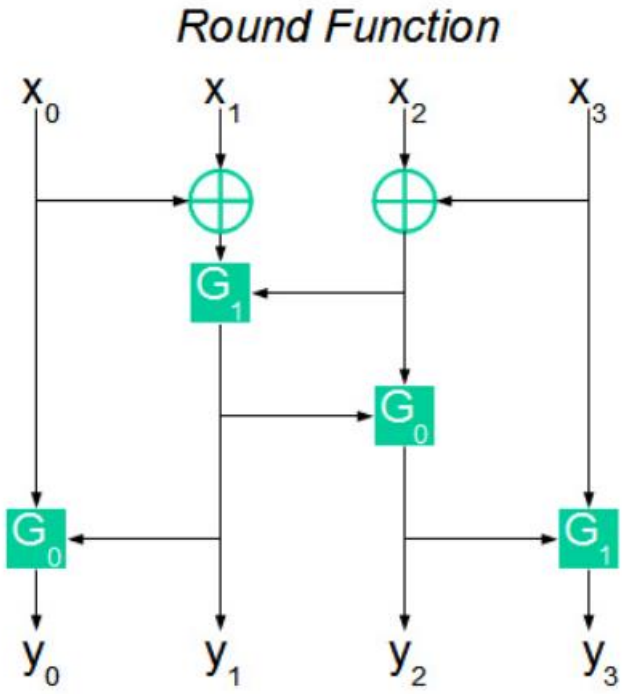

Рис.2 – функция F.

На входе функция F получает 4 байта X_1, X_2, X_3, X_4. Далее входные байты перемешиваются и проходят через функции G_0 или G_1. 4 байта полученных после вычисления функций G_x образуют 32-битную выходную последовательность функции F.

Функции G_0 и G_1 выполняют преобразование 16-битной входной последовательности в 8-битный результат.

Функцию G_0 можно выразить следующим образом: $G_0(a,b) = \big(a + b(mod\ 256)\big) \ll 2$, где << — циклический сдвиг влево.
В то время как функция G_1 имеет следующее определение: $G_1(a,b) = \big(a + b + 1(mod\ 256)\big) \ll 2$.

Расшифровка алгоритма происходит по такому же принципу. Собственно, шифротекст разбивается на левый и правый блок и все операции шифрования выполняются в обратном порядке.

Режим обратной связи по выходу

Схема шифрования в режиме OFB определяется следующим образом:

$$K_o = IV$$
$$K_i = E(K, K_{i-1}) \text{ для } i = 1, \ldots, n$$
$$C_i = K_i \oplus P_i$$

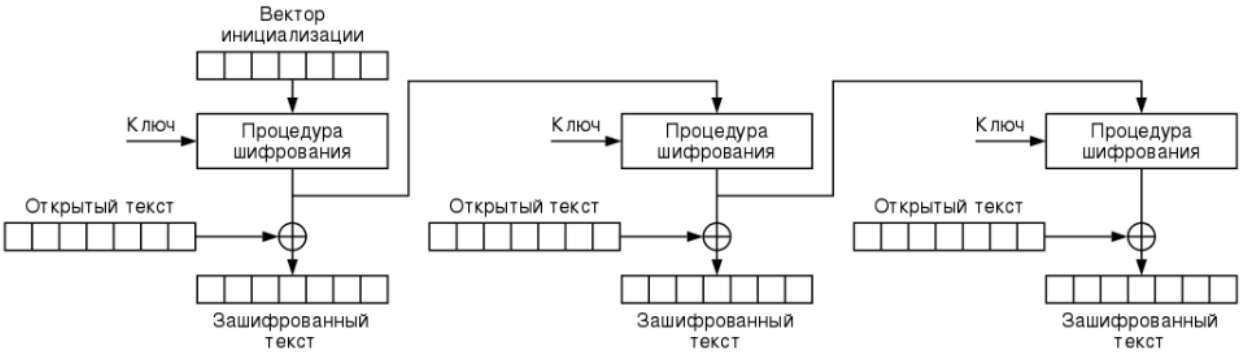

Рис.3 - Схема шифрования в режиме обратной связи по выходу (OFB).

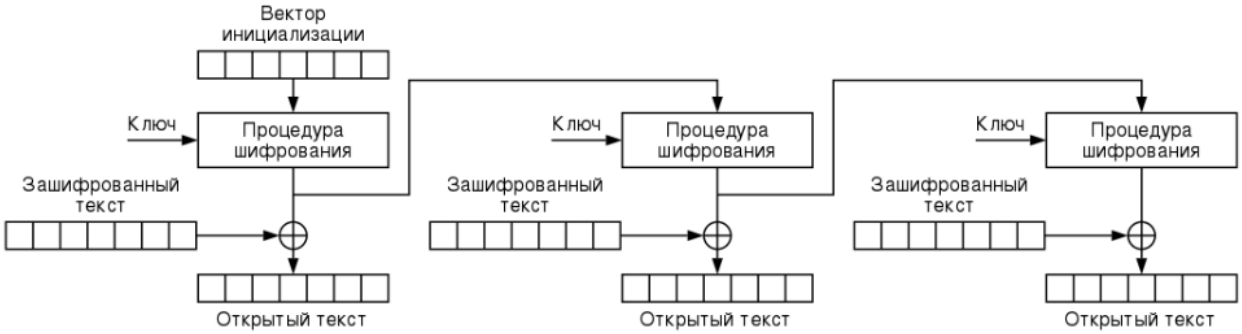

Рис.4 - Схема дешифрования в режиме обратной связи по выходу (OFB).

Особенности режима

- Значение вектора инициализации должно быть уникальным для каждой процедуры шифрования одним ключом. Его необязательно сохранять в секрете и оно может быть передано вместе с шифротекстом.
- Алгоритм дешифрования в режиме OFB полностью совпадает с алгоритмом шифрования. Функция дешифрования блочного алгоритма не используется в данном режиме, т.к. ключевой поток генерируется только функцией шифрования блока.
- Режим OFB наглядно демонстрирует одну из проблем потоковых шифров. При использовании одного и того же вектора инициализации для шифрования нескольких сообщений будет сгенерирован одинаковый поток ключей. Предположим, что P1 и P2 — два разных сообщения для шифрования ключом K. Зашифруем исходные сообщения в режиме OFB и получим два шифротекста — C1 и C2, соответственно. Таким образом,

будет справедливо следующее тождество:

$$C_1 \oplus C_2 = E(K, K_{i-1}) \oplus P_1 \oplus E(K, K_{i-1}) \oplus P_2 = P_1 \oplus P_2$$

Следовательно, если потенциальному злоумышленнику известна хотя бы одна пара шифрованного и открытого текста, вычисление любых открытых текстов, зашифрованных таким же ключом и с идентичным вектором инициализации, становится тривиальной задачей.

- Появление коллизии в ключевом потоке (или совпадение вектора инициализации и одного из ключевых блоков) приведёт к циклическому повторению ключевой последовательности, что может вызвать нарушение безопасности режима шифрования, как показано в предыдущем пункте.
- Распространение ошибки в данном режиме не происходит. Изменение одного бита в шифрованном тексте приведет к изменению одного бита при дешифровании. Однако, потеря бита в шифротексте приведет к некорректному дешифрованию всех последующих битов.

2. Пример работы программы:

Рис.5 – исходное изображение

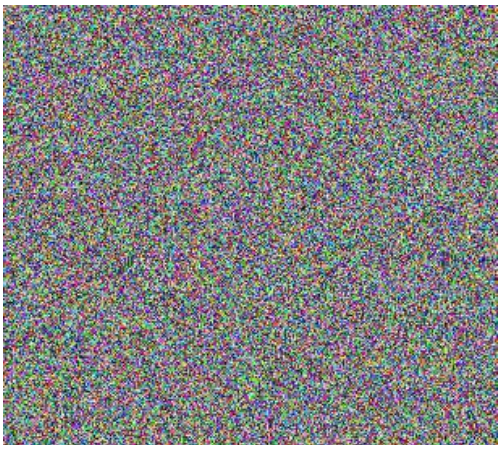

Рис.6 – закодированное изображение

Рис.7 – раскодированное изображение

3. Расчет коэффициента корреляции

Изменим в зашифрованном изображении 1 пиксель и заново раскодируем его:

Рис.8 – искаженное раскодированное изображение

Получим, что в результате изменения 1 пикселя, произошла замена других соседних пикселей в блоке, что повлекло некорректное раскодирование. Следовательно, можно говорить о взаимозависимости некоторых бит в данном алгоритме. Данное явление, при котором изменение одной величины влечет за собой изменение другой, называется корреляцией.

Коэффициент корреляции между j-м входным и k-м выходным битами узла замен вычисляется по формуле:

$$\rho_{jk} = \frac{\sum_{t=0}^{N-1} x_{tj} y_{tk} - \left(\sum_{t=0}^{N-1} x_{tj} \cdot \sum_{t=0}^{N-1} y_{tk}\right)/N}{\sqrt{\left(\sum_{t=0}^{N-1} x_{tj}^2 - \left(\sum_{t=0}^{N-1} x_{tj}\right)^2/N\right) \cdot \left(\sum_{t=0}^{N-1} y_{tk}^2 - left(\sum_{t=0}^{N-1} y_{tk}\right)^2/N}}. \quad \textbf{(1)}$$

Кроме того, для двоичных векторов xi, yi верна более простая формула:

$$\rho_{jk} = 1 - 2^{-(n-1)} \sum_{z=0}^{N-1} (x_{z,j} \oplus y_{z,k}). \quad \textbf{(2)}$$

Вычислим коэффициенты корреляции для следующего блока замен для алгоритма FEAL:

9 8 3 A C D 7 E 0 1 B 2 4 5 F 6

Получим битовые представления всех чисел нашей подстановки:

0000	1001
0001	1000
0010	0011
0011	1010
0100	1100
0101	1101
0110	0111
0111	1110
1000	0000
1001	0001
1010	1011
1011	0010
1100	0100
1101	0101
1110	1111
1111	0110

Таблица 1 – битовые представления чисел подстановки

В этой таблице число 0 (нумерация начинается с нуля) переходит в число 9, число 1 переходит в 8, 2 в 3, число 3 в 10, 4 в 12,..., число 15 переходит в 6 и тд.

Теперь, интерпретируя последовательность битов каждого разряда как множество значений случайной величины, вычислим коэффициенты корреляции между последовательностью входящих битов i-го разряда и последовательностью выходящих битов j-го разряда, i,j = 0,1, 2, 3.

j/k	0	1	2	3
0	-0.25	0	0	0
1	0	1	0	0
2	0	0	1	0
3	0	0	0	-0.5

Таблица 2 – расчитанные коэффициенты корреляции

Мы видим, что биты 1 и 2 группы остаются неизменными, что свидетельствует о взаимозависимости некоторых входных и выходных потоков данного блока.

4. Вывод

В ходе данной лабораторной работы был программно воспроизведен алгоритм шифрования FEAL. Исследован процесс распространения ошибок в реализуемом режиме шифрования, приведен пример распространения ошибок. Был вычислен коэффициент корреляции для входного и выходного потока алгоритма шифрования.

Можно выделить достоинства и недостатки алгоритма:
Достоинства:

- простота аппаратной реализации на современной электронной базе.
- простота программной реализации в силу того, что значительная часть функций поддерживается на аппаратном уровне в современных компьютерах (например, сложение по модулю 2).
- хорошая изученность алгоритмов, построенных на основе сетей Фейстеля.

Недостатки:

- за один раунд шифруется только половина входного блока.

5. Список источников

1. А.Л. Чмора "Современная прикладная криптография"
2. Черчхаус. Коды и шифры
3. НИУ ВШЭ (Высшая Школа Бизнес-Информатики): Криптографические методы защиты информации.