Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Московский государственный технический университет
имени Н. Э. Баумана
(национальный исследовательский университет)»
(МГТУ им. Н. Э. Баумана)

ФАКУЛЬТЕТ «Информатика и системы управления»

КАФЕДРА «Программное обеспечение ЭВМ и информационные технологии»

ОТЧЕТ

по лабораторной работе №2

по курсу «Защита информации»

на тему: «Симметричный алгоритм DES/3DES»

Вариант № 3 (PCBC)

Преподаватель _____ И. С. Чиж
(Подпись, дата) (И. О. Фамилия)

2023 г.

1 Теоретический раздел

DES (in English, Data Encryption Standard) — алгоритм для симметричного шифрования, разработанный фирмой IBM и утверждённый правительством США в 1977 году как официальный стандарт. Размер блока для DES равен 64 битам. В основе алгоритма лежит сеть Фейстеля с 16 циклами (раундами) и ключом, имеющим длину 56 бит. Алгоритм использует комбинацию нелинейных (S-блоки) и линейных (перестановки E, IP, IP^{-1}) преобразований. Для DES рекомендовано несколько режимов:

- ECB (electronic code book) — режим «электронной кодовой книги» (простая замена);
- CBC (cipher block chaining) — режим сцепления блоков;
- PCBC (propagating cipher block chaining) — режим распространяющегося сцепления блоков;
- CFB (cipher feed back) — режим обратной связи по шифротексту;
- OFB (output feed back) — режим обратной связи по выходу;
- Counter Mode (CM) — режим счётчика.

Прямым развитием DES в настоящее время является алгоритм Triple DES (3DES). В 3DES шифрование/расшифровка выполняются путём троекратного выполнения алгоритма DES.

1.1 Алгоритм DES

Алгоритм шифрования DES состоит из следующих шагов.

1. Совершить начальную перестановку с помощью функции IP.
2. Создать 16 ключей.
   (a) С помощью функции G провести удаление проверочных битов из ключа и провести перестановку. Получить 56-битный ключ из 64-битного блока.

(b) Разбить получившийся ключ на две половины C_0 (старшая) и D_0 (младшая).

(c) Для каждой итерации (от 1 до 16) совершить циклический сдвиг половин влево на величину, заданную в таблице. Величина зависит от номера итерации.

(d) Склеить половинки в 56-битный ключ.

(e) Провести перестановку и изменение размера ключа до 48 бит с помощью функции H.

3. Разбить блок на две половины по 32 бита L_0 (старшая) и R_0 (младшая).

4. На каждой итерации от 1 до 16 вычислить новые значения $L_i = R_{i-1}$ и $R_i = L_{i-1} \oplus f(R_{i-1}, K_i)$.

   (a) Провести перестановку с увеличение размера блока с 32 до 48 бит с помощью функции E.

   (b) Сложить получившийся блок по модулю 2 с ключом.

   (c) Разбить результат на 8 блоков по 6 бит.

   (d) Для каждого блока, получить номер строки, который представляет собой два бита — первый и последний биты блока из 6 бит.

   (e) Получить номер столбца, как 4 серединных бита.

   (f) По номеру строки и столбца, найти соответствующее значение функции S_i. Значение представляет собой 4-битное число.

   (g) Получить восемь 4-битных блоков.

   (h) Склеить блоки в 32-битный блок.

   (i) Провести перестановку с помощью функции P.

5. Совершить конечную перестановку с помощью функции IP^{-1}.

Расшифрование представляет собой тот же алгоритм, запущенный в обратном порядке.

1.2 Алгоритм PCBC

На рисунках 1.1–1.2 изображена схемы шифрования и расшифрования с использованием алгоритма PCBC.

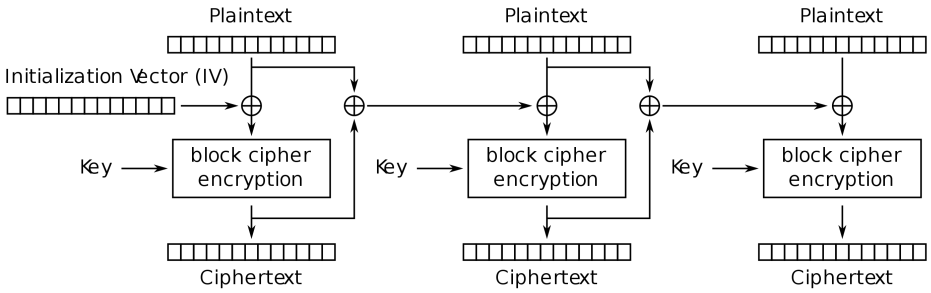

Рисунок 1.1 – Шифрование с использованием PCBC

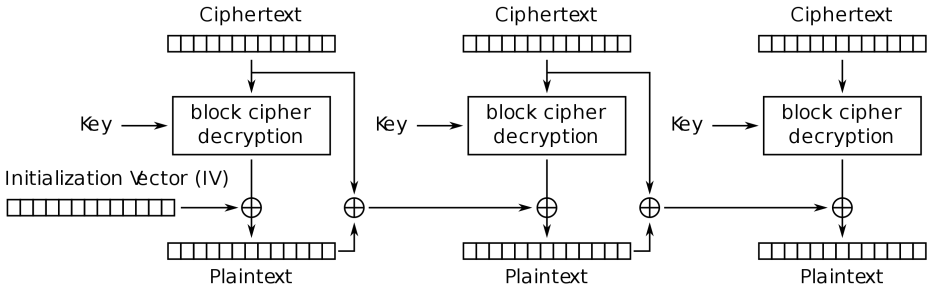

Рисунок 1.2 – Расшифрование с использованием PCBC

2 Практический раздел

2.1 Листинг алгоритма DES

2.2 Листинг алгоритма PCBC

2.3 Тестирование

ПРИЛОЖЕНИЕ А