Министерство образования Республики Беларусь

Учреждение образования

БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ

Факультет информационной безопасности

Кафедра защиты информации

Тема работы:

ГЕНЕРАЦИЯ РАУНДОВЫХ КЛЮЧЕЙ DES НА БАЗЕ БЛОКОВ LS

Вариант №17

Студент: Савченко Екатерина

Номер группы: 961401

Преподаватель: А.М. Тимофеев

Минск 2022

**Цель:** изучение схемы генерации раундовых ключей DES, построенной на базе блоков циклического сдвига влево *LS*.

**Краткие теоретические сведения.**

На рисунке 1 показана структурная схема генерации ключей DES, которая вырабатывает 16 раундовых ключей *ki* (*i* = 1, 2, …, 16).

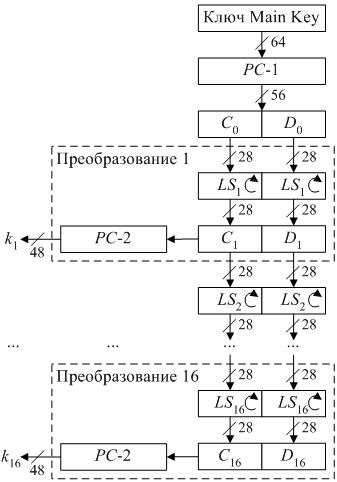


Рисунок 1 - Структурная схема генерации раундовых

ключей DES на базе блоков циклического сдвига влево *LS*

Каждый раундовый ключ *ki* состоит из 48 бит исходного секретного ключа Main Key. Ключ Main Key содержит 56 значащих бит и 8 проверочных бит для контроля на четность, расположенными в позициях 8, 16, 24, 32, 40, 48, 56, 64. Для удаления контрольных битов и подготовки ключа к работе используется функция первоначальной подготовки ключа *PC*-1, поясняемая рисунком 2.

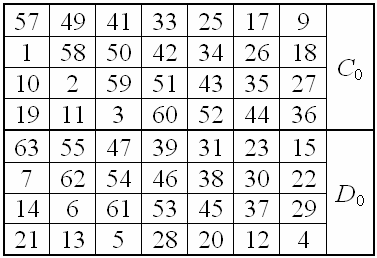


Рисунок 2 - Функция первоначальной подготовки ключа *PC*-1

Как видно из рисунка 2, функция *PC*-1разделена на две части: *С*0 и *D*0 по 28 бит каждая. Первые четыре строки матрицы *PC*-1 определяют, как выбираются биты последовательности *С*0 (первым битом *С*0 будет бит 57 ключа Main Key, затем бит 49 и т.д., а последними битами - биты 44 и 36), а следующие четыре строки - биты последовательности *D*0 (первым битом *D*0 будет бит 63 ключа Main Key, затем бит 55 и т.д., а последними битами - биты 12 и 4).

После определения *С*0 и *D*0 рекурсивно определяются *Сi* и *Di* путем циклического сдвига влево на один или два бита *Сi* - 1 и *Di* - 1 соответственно в зависимости от номера преобразования, как показано в таблице 1.

Таблица 1 - Количество сдвигов для вычисления раундовых ключей



Операции циклического сдвига влево выполняются для последовательностей *Сi* и *Di* независимо (см. рисунок 1). Например, последовательность *С*5 получается посредством циклического сдвига влево на две позиции последовательности *С*4, последовательность *D*5 - посредством сдвига влево на две позиции последовательности *D*4, а *С*16 и *D*16 получаются из *С*15 и *D*15 посредством циклического сдвига влево на одну позицию (см. таблицу 1).

Раундовый ключ *ki*, определяемый на каждом преобразовании (см. рисунок 1), есть результат выбора конкретных битов из 56-битовой последовательности *CiDi* и их перестановки, что реализуется функцией, завершающей подготовку ключа *PC*-2, поясняемая рисунком 3.

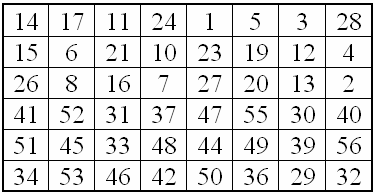


Рисунок 3 - Функция, завершающая подготовку ключа *PC*-2

Как видно из рисунка 3, первым битом ключа раундового ключа *ki*, будет 14-ый бит последовательности *CiDi*, вторым - 17-ый бит, и т.д., а последним - 32-ой бит.

**Полученные результаты практических расчетов:**

– раундовый ключ (подключ) *k*1 = EEB92C85A27B;

– раундовый ключ (подключ) *k*2 = 8395E7F147C9;

– раундовый ключ (подключ) *k*3 = F942D75A920F;

***результаты, полученные средствами автогенерации учебного модуля:***

– раундовый ключ (подключ) *k*4 = 35D3A8D675AC;

– раундовый ключ (подключ) *k*5 = 9211F7283BE9;

– раундовый ключ (подключ) *k*6 = BD4A55F2F833;

– раундовый ключ (подключ) *k*7 = 0773AC670F3A;

– раундовый ключ (подключ) *k*8 = 9A15F59D395A;

– раундовый ключ (подключ) *k*9 = 5BCC13DD0765;

– раундовый ключ (подключ) *k*10 = 6DA9BADACAC8;

– раундовый ключ (подключ) *k*11 = B6A48F50F71D;

– раундовый ключ (подключ) *k*12 = 7B0E12BB34A8;

– раундовый ключ (подключ) *k*13 = 6CB8BCE87B23;

– раундовый ключ (подключ) *k*14 = 96A45E366A3E;

– раундовый ключ (подключ) *k*15 = 6E4E32F519D2;

– раундовый ключ (подключ) *k*16 = 75F321CFA394.

**Контрольные вопросы:**

1 Для чего используется схема генерации криптографических подключей DES, построенная на базе блоков циклического сдвига влево *LS*?\

*Алгоритм LS используется для шифрования, в отличие от RS, который используется для ускорения процесса расшифрования*

2 Какова длина в битах одного подключа DES в схеме генерации криптографических подключей DES, построенной на базе блоков циклического сдвига влево *LS*?

*Каждый раунд использует различные сгенерированные 48-битовые подключи.*

3 Сколько байт имеет основной ключ DES?

*Основной ключ – 56 бит (7 байт)*

4 Какие математические операции используются в схеме генерации криптографических подключей DES, построенной на базе блоков циклического сдвига влево *LS*?

*Замена, перемешивание, сложение по модулю 2 (операция XOR)*

5 Насколько сложными для современных программных и программно-аппаратных средств являются математические операции, используемые в схеме генерации криптографических подключей DES, построенной на базе блоков циклического сдвига влево *LS*?

*Алгоритм использует только стандартную арифметику 64-битовых чисел и логические операции, поэтому легко реализуется на аппаратном уровне.*

**Выводы по результатам выполнения работы:**

В результате лабораторной работы я изучила схему генерации раундовых ключей DES, построенную на базе блоков циклического сдвига влево *LS*.Также были обнаружены преимущества алгоритма DES:использование только одного ключа 56 бит, относительную простоту алгоритма и высокую скорость обработки, для шифрования и расшифрования возможность использования разных пакетов программ, соответствующих DES, высокая стойкость алгоритма.

**Отчет сформирован (не удалять!!! не изменять!!!):**

1 Дата и время: 23.09.2022 13:26;

2 Вариант №: 17;

3 Студент: Савченко Екатерина;

4 Номер группы: 961401;

5 Допущено ошибок 1:

– практическая часть: 0;

– тестовое задание: 1.

**Коды аутентификации (не удалять!!! не изменять!!!):**

1 Учебного модуля: 60486081BB94D368152932073DD85FC9;

2 Студента: 0053AF406311F1A600B088749D2E3612;

3 Результатов: 20EEAC58476E2ACBB1856C67BC8668CA.