Лабораторная работа №2
«Алгоритм симметричного шифрования S-DES»

1. Цель работы:

Изучение работы простейшего алгоритма симметричного шифрования S-DES.

2. Основные теоретические сведения:

Упрощенный DES - это алгоритм шифрования, имеющий, скорее, учебное, чем практическое значение. По свойствам и структуре он подобен DES, но имеет гораздо меньше параметров. Данный алгоритм был разработан профессором Эдвардом Шейфером (Edward Schaefer) из Университета Санта-Клара.

На рис. 1 показана общая структура упрощенного алгоритма S-DES. Данный алгоритм получает на входе 8-битовый блок открытого текста и 10-битовый ключ, а на выходе генерируется 8-битовый блок шифрованного текста. Алгоритм дешифрования S-DES в качестве исходных данных использует 8-битовый блок шифрованного текста и тот же 10-битовый ключ, который применялся для шифрования, а в результате работы алгоритм дешифрования должен генерировать 8-битовый блок открытого текста.

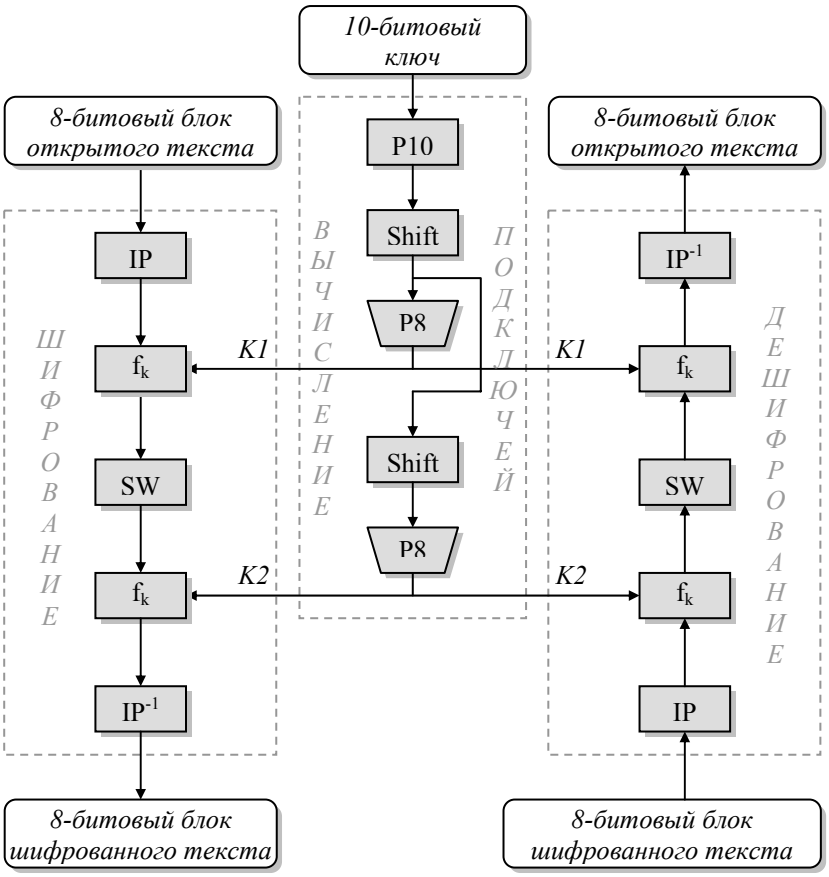

Рис. 1. Структура упрощенного алгоритма S-DES

Алгоритм шифрования включает последовательное выполнение пяти операций:

- начальной перестановки IP,
- сложной функции f_K, являющейся композицией операций перестановки и подстановки и зависящей от полученного ключа,
- перестановки SW, при которой две половинки последовательности данных просто меняются местами,
- еще раз функции f_K,
- перестановки, обратной начальной (IP^{-1}).

Данный алгоритм можно представить в виде:

$$\textit{шифрованный текст} = IP^{-1}\,(\,f_{K2}\,(\,SW\,(\,f_{K1}\,(\,IP\,(\,\textit{открытый текст}\,)\,)\,)\,)\,),$$
$$\textit{открытый текст} = IP^{-1}\,(\,f_{K1}\,(\,SW\,(\,f_{K2}\,(\,IP\,(\,\textit{шифрованный текст}\,)\,)\,)\,)\,).$$

где

$$K_1 = P8\,(\,Shift\,(\,P10\,(\textit{ключ})\,)\,),\quad K_2 = P8\,(\,Shift\,(\,Shift\,(\,P10\,(\textit{ключ})\,)\,)\,).$$

2.1. Вычисление ключей S-DES

В алгоритме S-DES используется 10-битовый ключ, который должен быть как у отправителя, так и у получателя сообщения. Из этого ключа на определенных этапах шифрования и дешифрования генерируется два 8-битовых подключа. На рис. 2 показана схема процедуры создания этих подключей.

Сначала выполняется перестановка битов ключа следующим образом. Если 10-битовый ключ представить в виде (k_1 , k_2, k_3, k_4, k_5, k_6, k_7, k_8, h_9, h_{10}), то перестановку P10 можно задать формулой:

$P10(k_1, k_2, k_3, k_4, k_5, k_6, k_7, k_8, h_9, h_{10}) = (k_3, k_5, k_2, k_7, k_4, h_{10}, k_1, h_9, k_8, k_6)$.

Можно также представить перестановку P10 в следующей табличной форме.

P10									
3	5	2	7	4	10	1	9	8	6

После этого отдельно для первых пяти битов и отдельно для вторых выполняется циклический сдвиг влево LS-1, который еще называют вращением.

Затем применяется перестановка P8, в результате которой из 10-битового ключа сначала выбираются, а затем переставляются 8 битов по следующему правилу.

P8							
6	3	7	4	8	5	10	9

В результате этой операции получается первый подключ K_1.

Теперь нужно вернуться к двум 5-битовым строкам, полученным в результате применения функций LS-1, и выполнить с каждой из этих строк циклический сдвиг влево на две позиции LS-2.

Наконец, применив к полученной в результате последовательности перестановку P8, получим подключ K_2.

Например:

```
Ключ       : 1011001001
После  P10: 1001111000
После LS-1: 0011110001   ->  После P8 (K1): 11010110
После LS-2: 1110000110   ->  После P8 (K2): 01001001
```

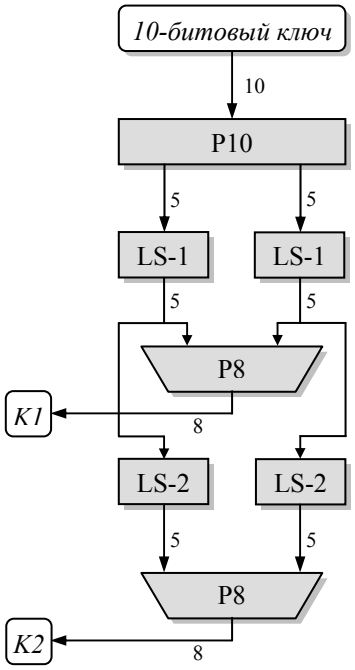

Рис. 2. Вычисление подключей

2.2. Шифрование S-DES

На рис. 3 представлена более подробная схема алгоритма шифрования S-DES. Как уже упоминалось, процесс шифрования представляет собой последовательное выполнение пяти операций.

2.2.1. Начальная и завершающая перестановки

На вход алгоритма поступает 8-битовый блок открытого текста, к которому применяется начальная перестановка, заданная функцией IP.

IP							
2	6	3	1	4	8	5	7

Все 8 битов открытого текста сохраняют свои значения, но меняется порядок их следования. На завершающей стадии алгоритма выполняется обратная перестановка.

IP^{-1}							
4	1	3	5	7	2	8	6

Как легко убедиться с помощью простой проверки, вторая из приведенных выше перестановок действительно является обратной по отношению к первой, т.е. $IP^{-1}(IP(X)) = X$.

2.2.2. Функция f_K

Самым сложным компонентом S-DES является функция f_K, представляющая собой комбинацию перестановки и подстановки. Первой операцией является операция расширения/перестановки последних четырех входных битов.

E/P							
4	1	2	3	2	3	4	1

Затем к полученному значению с помощью операции XOR добавляется 8-битовый подключ.

Первые четыре бита поступают на вход модуля S0, на выходе которого получается 2-битовая последовательность, а оставшиеся четыре бита — на вход модуля S1, на выходе которого получается другая 2-битовая последовательность. Модули S0 и S1 можно определить так:

$$S0 = \begin{array}{c} \\ 0 \\ 1 \\ 2 \\ 3 \end{array} \begin{array}{c} \begin{array}{cccc} 0 & 1 & 2 & 3 \end{array} \\ \begin{bmatrix} 1 & 0 & 3 & 2 \\ 3 & 2 & 1 & 0 \\ 0 & 2 & 1 & 3 \\ 3 & 1 & 3 & 1 \end{bmatrix} \end{array}, \quad S1 = \begin{array}{c} \\ 0 \\ 1 \\ 2 \\ 3 \end{array} \begin{array}{c} \begin{array}{cccc} 0 & 1 & 2 & 3 \end{array} \\ \begin{bmatrix} 1 & 1 & 2 & 3 \\ 2 & 0 & 1 & 3 \\ 3 & 0 & 1 & 0 \\ 2 & 1 & 0 & 3 \end{bmatrix} \end{array}$$

Эти S-модули (матрицы кодирования) работают следующим образом. Первый и четвертый биты входной последовательности рассматриваются как 2-битовые числа, определяющие строку, а второй и третий — как числа, определяющие столбец S-матрицы. Элементы, находящиеся на пересечении соответствующих строки и столбца, задают 2-битовые выходные значения. Например, если первые четыре бита равны (0100), то выходные 2 бита задаются значением, которое находится на пересечении строки 0 (00) и столбца 2 (10) матрицы S0 (оно равно 3 или (11) в двоичном представлении).

Теперь 4 бита, полученные на выходе модулей S0 и S1, преобразуются с помощью перестановки P4 следующим образом.

P4			
2	4	3	1

Результат применения перестановки P4 добавляется к первым четырем входным битам с помощью операции XOR. Полученный результат и является значением функции f_K.

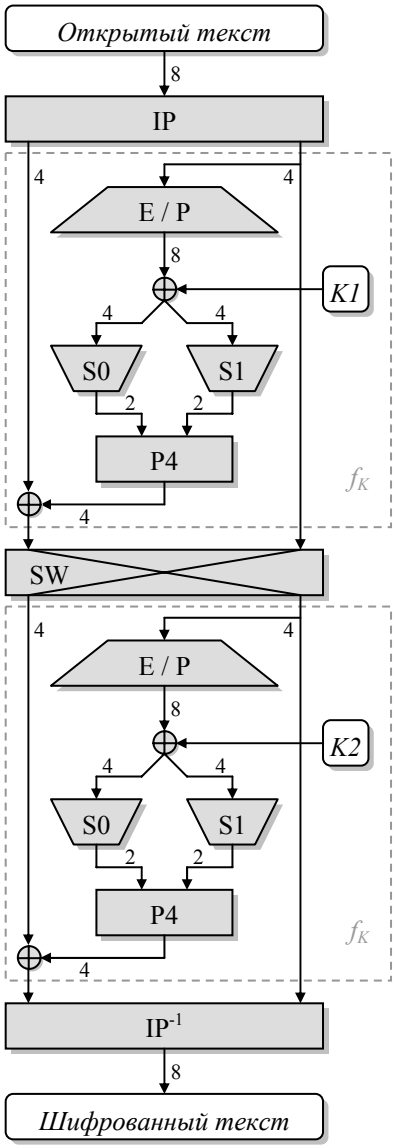

Рис. 3. Алгоритм S-DES

2.2.3. Функция-переключатель

Функция f_K изменяет только четыре левых бита. Поэтому следующей операцией в алгоритме шифрования является использование функции SW, которая меняет местами первые и последние четыре бита последовательности, чтобы при следующем вызове функции f_K последняя работала уже с другой четверкой битов. При втором вызове f_K функции E/P, S0, S1 и P4 остаются теми же, что и при первом, но вместо ключа K_1, используется ключ K_2.

Например:

```
Открытый текст: 1101 1010
После      I/P: 1001 1011
После      E/P:    11010111
После XOR с K1:    00000001
После   матриц:      01  10
После       P4:       1010
XOR с левыми 4: 0011
После      fk1: 0011 1011
После       SW: 1011 0011
После      E/P:    10010110
После XOR с K2:    11011111
После   матриц:      11  11
После       P4:       1111
XOR с левыми 4: 0100
После      fk2: 0100 0011
После    I/P-1: 0000 1110
Шифров.  текст: 0000 1110
```

3. Задание на лабораторную работу

Необходимо зашифровать с помощью алгоритма S-DES первые пять букв своей фамилии.

3.1. Порядок выполнения:

1. Взять первые 10 букв своих «ФамилияИмяОтчество».
2. Преобразовать их в 10-битный ключ по следующей схеме: каждая согласная буква заменяется на «1», а гласная на «0» (к гласным буквам относятся: а, я, у, ю, и, ы, о, ё, э, е; к согласным все остальные).
3. По известному алгоритму высчитать два подключа.
4. Взять первые пять букв своих «ФамилияИмяОтчество».
5. По приведенной ниже кодовой таблице ASCII, заменить каждую букву на соответствующий код (с учетом регистра).
6. Перевести каждый код в двоичное 8-битное представление.
7. Провести алгоритм S-DES для каждого 8-битного блока.
8. Полученные пять 8-битных шифрованных блока преобразовать в десятичный формат, которые и будут служить ответом.

Кодовая таблица ASCII					
А = 128	а = 160	К = 138	к = 170	Х = 149	х = 229
Б = 129	б = 161	Л = 139	л = 171	Ц = 150	ц = 230
В = 130	в = 162	М = 140	м = 172	Ч = 151	ч = 231
Г = 131	г = 163	Н = 141	н = 173	Ш = 152	ш = 232
Д = 132	д = 164	О = 142	о = 174	Щ = 153	щ = 233
Е = 133	е = 165	П = 143	п = 175	Ъ = 154	ъ = 234
Ё = 240	ё = 241	Р = 144	р = 224	Ы = 155	ы = 235
Ж = 134	ж = 166	С = 145	с = 225	Ь = 156	ь = 236
З = 135	з = 167	Т = 146	т = 226	Э = 157	э = 237
И = 136	и = 168	У = 147	у = 227	Ю = 158	ю = 238
Й = 137	й = 169	Ф = 148	ф = 228	Я = 159	я = 239

3*. Дополнительное задание на лабораторную работу.

1. Составить программу на языке высокого уровне (Pascal, C++), реализующую алгоритм шифрования S-DES, шифрующую буквы и символы, вводимые с клавиатуры.
2. Составить программу на языке высокого уровне (Pascal, C++), реализующую алгоритм шифрования S-DES, шифрующую файлы.

4. Содержание отчета

1. «ФамилияИмяОтчество».
2. 10-битовый ключ.
3. 2 подключа.
4. Пять 8-битовых блока.
5. Пять шифрованных блока.