Реферат на тему:

**Спрощений Data Encryption Standart**

На рисунку 1 наведена структура спрощеної схеми шифрування DES (Data Encryption Standart). На вхід схеми кодування подається 8 бітовий відкритий текст та 10 бітовий ключ. Результатом роботи схеми є 8 бітовий шифротекст. Схема декодування приймає на вхід 8 бітовий шифротекст та 10 бітовий ключ та виробляє на виході 8 бітовий відкритий текст.

# IP

8 бітовий

відкритий текст

# fK

# SW

# fK

# IP-1

8 бітовий

шифротекст

# P8

# Зсув

# P10

10 бітовий

ключ

# Зсув

# P8

# IP

8 бітовий

відкритий текст

# fK

# SW

# fK

# IP-1

8 бітовий

шифротекст

K1

K2

K2

K1

**кодування**

**декодування**

Рисунок 1. Спрощена схема DES

Алгоритм кодування складається із 5 функцій: початкової перестановки IP, функції fK, яка включає в себе як перестановку так і заміну, просту перестановку SW, яка переставляє праву та ліву частини даних, знову функцію fK, та кінцеву перестановку IP-1. Алгоритм кодування можна записати наступним чином:

шифротекст = IP-1 (fK2 (SW (fK1 (IP (відкритий текст)))))

При цьму ключі K1 та K2 визначаються як

K1 = P8 (Зсув (P10 (ключ))),

K2 = P8 (Зсув (Зсув (P10 (ключ))))

Алгоритм декодування має вигляд:

відкритий текст = IP-1 (fK1 (SW (fK2 (IP (шифротекст)))))

## Генерація ключа

Перестановка P10 має вигляд: (3, 5, 2, 7, 4, 10, 1, 9, 8, 6), тобто

P10(k1, k2, k3, k4, k5, k6, k7, k8, k9, k10) = (k3, k5, k2, k7, k4, k10, k1, k9, k8, k6)

Перестановка P8 визначається як (6, 3, 7, 4, 8, 5, 10, 9).

K2

K1

5

### P10

10 бітовий ключ

10

10

5

### LS-1

### LS-1

5

5

### P8

8

### LS-2

### LS-2

5

5

### P8

8

Рисунок 2. Генерація ключів

Блок LS-1 виконує циклічний зсув вліво на 1 біт, а блок LS-2 – циклічний зсув вліво на 2 біти.

## Алгоритм кодування

Вхідний відкритий 8 бітовий текст спочатку подається на перестановку IP:

IP = (2, 6, 3, 1, 4, 8, 5, 7)

В кінці алгоритму буде використана обернена перестановка IP-1:

IP-1 = (4, 1, 3, 5, 7, 2, 8, 6)

При цьому справедлива рівність: IP-1 ( IP(X)) = X

4

4

4

4

4

8

2

2

4

K1

8

IP

8

E / P

8

S0

4

S1

P4

4

8

2

2

4

K2

8

E / P

8

S0

4

S1

P4

4

4

IP-1

відкритий текст

шифротекст

8

4

fK

4

fK

SW

F

F

Рисунок 3. Детальна схема шифрування DES

Функція fK є комбінацією функцій перестановки та заміни. Позначимо через Lта R ліві та відповідно праві 4 біти 8 - бітового входу до fK. Якщо позначити через F відображення 4 бітових слів у 4 бітові (не обов’язкого взаємно однозначне), то функцію fK можна визначити так:

fK (L, R) = (L F(R, Ki), R)

Опишемо структуру відображення F. Блок розширення / перестановки E/P, який на вхід приймає 4 бітове число, має вигляд E / P = (4, 1, 2, 3, 2, 3, 4, 1). Після операції XOR результату блоку E / P з одним із підключей, ліві 4 біти подаються на таблицю S0, а праві 4 біти – на матрицю S1.

На вхід S матриці подається 4 бітове число. Перший та четвертий біти утворюють двобітове число – номер рядка, а другий та третій біти – номер стовпчика. Наприклад, якщо на вхід матриці S1 подається 1011, то знаходимо число, яке знаходиться в матриці S1 на перетині рядка 11 (третій) та стовпчика 01 (перший). Це число 1 (нумерація рядків та стовпчиків починається з 0). Результатом проходження інформації через S матрицю є двобітове число. Отже S1(1011) = 01.

S0 =  S1 = 

Результат роботи S матриць подається на перестановку P4 = (2, 4, 3, 1).

Функція SW міняє місцями праві та ліві 4 біти.

**Структура S матриці**

Нехай S(a, b, c, d) = (q, r). q та r є нелінійними функціями від a, b, c, d. Наприклад, в матриці S0 результуючі біти зв’язані з вхідними наступними нелінійними рівняннями:

q = abcd + ab + ac + b + d

r = abcd + abd + ab + ac + ad + a + c + 1