Таблицы замен и перестановок:

S_{24} = [9, 12, 15, 1, 0, 2, 10, 8, 14, 7, 6, 3, 11, 13, 4, 5]

P_{24} = [15, 8, 0, 13, 6, 5, 14, 9, 2, 11, 10, 3, 7, 12, 4, 1]

Таблица линейных приближений блока замены:

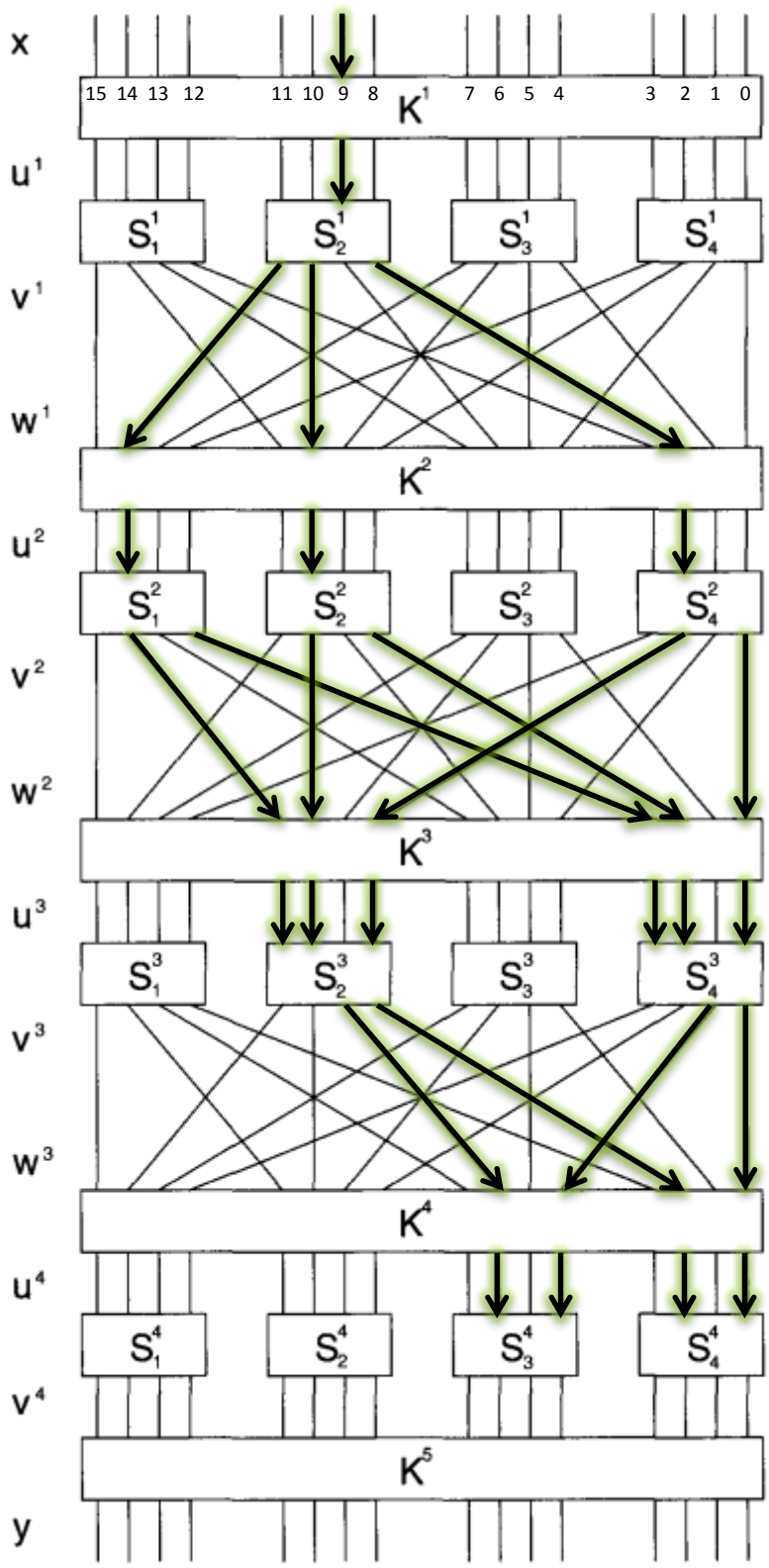
	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	2	-2	0	0	-2	2	0	-2	4	4	2	-2	0	0	2
2	0	0	0	0	0	0	0	0	-2	2	-2	2	2	6	2	-2
3	0	-2	2	0	4	-2	2	4	0	-2	2	0	0	2	-2	0
4	0	-2	-2	0	-2	-4	4	-2	0	-2	-2	0	2	0	0	2
5	0	0	0	-4	-2	2	2	2	-2	2	-2	-2	0	0	-4	0
6	0	2	2	0	-2	0	0	-2	-2	-4	0	2	-4	2	-2	0
7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

Рассмотрим на примере, как рассчитываются значения в этой таблице на примере случайной величины с максимальным отклонением. Рассматривается значение T(2, 13) = 6, тогда случайная величина будет равна: $x_3 \oplus y_1 \oplus y_2 \oplus y_4$.

x1	x2	x3	x4	y1	y2	y3	y4	$x_3 \oplus y_1 \oplus y_2 \oplus y_4$
0	0	0	0	1	0	0	1	0
0	0	0	1	1	1	0	0	0
0	0	1	0	1	1	1	1	0
0	0	1	1	0	0	0	1	0
0	1	0	0	0	0	0	0	0
0	1	0	1	0	0	1	0	0
0	1	1	0	1	0	1	0	0
0	1	1	1	1	0	0	0	0
1	0	0	0	1	1	1	0	0
1	0	0	1	0	1	1	1	0
1	0	1	0	0	1	1	0	0
1	0	1	1	0	0	1	1	0
1	1	0	0	1	0	1	1	0
1	1	0	1	1	1	0	1	1
1	1	1	0	0	1	0	0	0
1	1	1	1	0	1	0	1	1

По формуле: $N_L - 8 = 14 - 8 = 6$ – совпадает со значением таблицы.

Построим линейное приближение шифра:



$S_2^1: T_1 = u_9^1 \oplus v_{11}^1 \oplus v_{10}^1 \oplus v_8^1$

$S_1^2: T_2 = u_{14}^2 \oplus v_{14}^2 \oplus v_{12}^2$

$S_2^2: T_3 = u_{10}^2 \oplus v_{10}^2 \oplus v_8^2$

$S_4^2: T_4 = u_2^2 \oplus v_2^2 \oplus v_0^2$

$S_2^3: T_5 = u_{11}^3 \oplus u_{10}^3 \oplus u_8^3 \oplus v_8^3 \oplus v_9^3$

$S_4^3: T_6 = u_3^3 \oplus u_2^3 \oplus u_0^3 \oplus v_1^3 \oplus v_0^3$

Из этого следует:

$T_1 = x_9 \oplus K_9^1 \oplus v_{11}^1 \oplus v_{10}^1 \oplus v_8^1$

$T_2 = v_{11}^1 \oplus K_{14}^2 \oplus v_{14}^2 \oplus v_{12}^2$

$T_3 = v_{10}^1 \oplus K_{10}^2 \oplus v_{10}^2 \oplus v_8^2$

$T_4 = v_8^1 \oplus K_2^2 \oplus v_2^2 \oplus v_0^2$

$T_5 = v_{14}^2 \oplus v_{10}^2 \oplus v_2^2 \oplus K_{11}^3 \oplus K_{10}^3 \oplus K_8^3 \oplus v_8^3 \oplus v_9^3$

$T_6 = v_{12}^2 \oplus v_8^2 \oplus v_0^2 \oplus K_3^3 \oplus K_2^3 \oplus K_0^3 \oplus v_0^3 \oplus v_1^3$

Получается случайная величина:

$x_9 \oplus v_0^3 \oplus v_1^3 \oplus v_8^3 \oplus v_9^3 \oplus K_9^1 \oplus K_{14}^2 \oplus K_2^2 \oplus K_{11}^3 \oplus K_{10}^3 \oplus K_8^3 \oplus K_3^3 \oplus K_2^3 \oplus K_0^3$

Из которой следует:

$x_9 \oplus u_0^4 \oplus u_2^4 \oplus u_4^4 \oplus u_6^4 \oplus$

$\oplus K_0^4 \oplus K_2^4 \oplus K_4^4 \oplus K_6^4 \oplus K_9^1 \oplus K_{14}^2 \oplus K_2^2 \oplus K_{11}^3 \oplus K_{10}^3 \oplus K_8^3 \oplus K_3^3 \oplus K_2^3 \oplus K_0^3$

Теперь будем вычислять значение: $x_9 \oplus u_0^4 \oplus u_2^4 \oplus u_4^4 \oplus u_6^4$.

Программа:

```
ssize = 256
count = [0 for i in range(ssize)]
for k1 in range(ssize):
    for j in range(0, len(plaintext)):
        x = plaintext[j]
        y = ciphertext[j]

        l1 = (k1 >> 4) & 15
        l2 = k1 & 15

        y_1 = (y >> 4) & 15
        y_2 = y & 15

        v_1 = y_1 ^ l1
        v_2 = y_2 ^ l2

        u_1 = e.asbox(v_1)
        u_2 = e.asbox(v_2)

        if grab(x, 9) ^ grab(u_1, 0) ^ grab(u_1, 2) ^ grab(u_2, 0) ^ grab(u_2, 2) == 0:
            count[k1] += 1
```

Результат – верно определены последние 8 бит пятого раундового ключа:

```
RESULT: 62, deviation: 951.0, bias: 0.023775
(L1, L2)=(3, 14) = (0011, 1110)
k5=1101011000111110
----------------------
```