به نام ایزد یکتا

درس رمزنگاری پیشرفته

استاد درس: دکتر محمود سلماسی‌زاده

تمرین ۱) برای مشخصه‌ی تفاضلی[۱] سه دوری الگوریتم DES، که در جدول زیر مطرح شده است[۲]، احتمال برقراری تفاضل در هر دور و در نهایت احتمال مشخصه (P) را محاسبه کنید. (برای این کار از جدول‌های مطرح شده در انتهای تمرین استفاده نمایید.)

$L'_0 = 0x00200008$ $L'_1 = 0x00000400$	$R'_0 = 0x00000400$ $R'_1 = 0x00000000$	$p_1 = ?$
$L'_1 = 0x00000400$ $L'_2 = 0x00000000$	$R'_1 = 0x00000000$ $R'_2 = 0x00000400$	$p_2 = ?$
$L'_2 = 0x00000000$ $L'_3 = 0x00000400$	$R'_2 = 0x00000400$ $R'_3 = 0x00200008$	$p_3 = ?$

$P = ?$

تمرین ۲) برای مشخصه‌ی تفاضلی دو دوری الگوریتم DES، که در جدول زیر مطرح شده است، احتمال مشخصه را محاسبه کنید.

$L'_0 = 0x19600000$ $L'_1 = 0x00000000$	$R'_0 = 0x00000000$ $R'_1 = 0x19600000$	$p_1 = ?$
$L'_1 = 0x00000000$ $L'_2 = 0x19600000$	$R'_1 = 0x19600000$ $R'_2 = 0x00000000$	$p_2 = ?$

$P = ?$

[۱] differential characteristic

[۲] مقادیر تفاضل‌ها، به صورت کدهای Hex بیان شده است.

تمرین ۳) با کمک مشخصه‌ی تفاضلی دو دوری الگوریتم DES، که در جدول بالا مطرح شده است، یک مشخصه‌ی ۱۳ دوری تولید کرده و احتمال آن را محاسبه نمایید. (در صورتی که دو مشخصه تفاضلی ۱۳ دوری می‌توان ساخت، جواب این سوال مشخصه‌ی دارای بیشترین احتمال است.)

تمرین ۴) می‌خواهیم با کمک مشخصه‌ی تفاضلی یک دوری مطرح شده در جدول زیر، الگوریتم ۴ دوری DES را تحلیل کنیم.

$L'_0 = 0x20000000$ $L'_1 = 0x00000000$	$R'_0 = 0x00000000$ $R'_1 = 0x20000000$	$p_1 = 1$

a) اگر δ یک مقدار Hex دلخواه باشد، نشان دهید:

$R'_2 = P(0x\delta 0000000)$

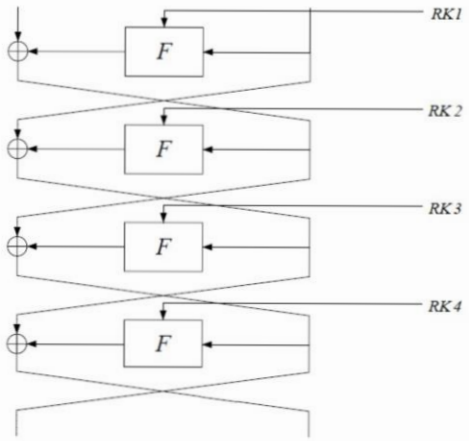
b) اگر مقدار زیرکلید دور چهارم را به صورت، $\mathsf{RK_4} = \mathsf{J_1}||\mathsf{J_2}||\mathsf{J_3}||\cdots||\mathsf{J_8}$ نمایش دهیم، نشان دهید:

$\forall j, 2 \leq j \leq 8; J_j \in \mathsf{test_j}\Big(Ej(L_4), E_j(L''_4), C'_j\Big)$

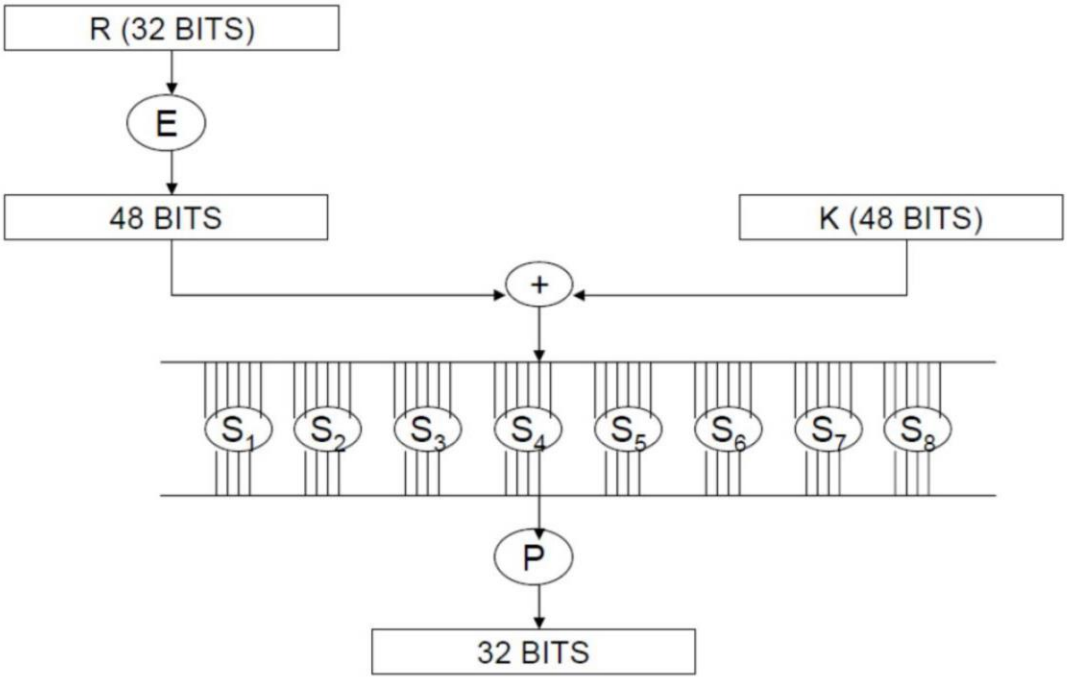
$C' = C'_1||C'_2||\cdots C'_8 = P^{-1}(R'_4)$

==========

شکل‌های مربوط به ساختار الگوریتم DES



شکل ۱: الگوریتم چهار دوری DES



شکل ۲: ساختار تابع F برای الگوریتم DES

ساختار تابع E

تابع E یک تابع با ورودی ۳۲ بیت و خروجی ۴۸ بیت است، که خروجی تکرار بعضی از بیت‌های ورودی است. شکل زیر جدول خروجی تابع را بر حسب مکان بیت‌های ورودی نمایش می‌دهد. به عنوان مثال بیت اول خروجی، بیت سی‌و دوم ورودی و بیت دوم خروجی، بیت اول ورودی است.

32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

شکل ۳: جدول تابع E

ساختار تابع P

تابع P یک تابع حافظ طول است که مکان بیت‌ها را تغییر می‌دهد (تابع جایگشتی). شکل زیر جدول خروجی تابع را بر حسب مکان بیت‌های ورودی نمایش می‌دهد. به عنوان مثال بیت اول خروجی، بیت شانزدهم ورودی و بیت دوم خروجی، بیت هفتم ورودی است.

16	7	20	21
29	12	28	17
1	15	23	26
5	18	31	10
2	8	24	14
32	27	3	9
19	13	30	6
22	11	4	25

شکل ۴: جدول تابع P

جدول‌های توزیع تفاضل ورودی و خروجی Sbox

این جدول‌ها که برای Sboxهای الگوریتم DES تدوین شده‌اند، نشان می‌دهد از ۶۴ حالت ممکن برای یک تفاضل ورودی معین، چند حالت به تفاضل خروجی معین نگاشته می‌شود. هشت جدول توزیع در صفحات بعد قرار گرفته‌اند.

Input XOR	Output XOR															
	0_x	1_x	2_x	3_x	4_x	5_x	6_x	7_x	8_x	9_x	A_x	B_x	C_x	D_x	E_x	F_x
0_x	64	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1_x	0	0	0	6	0	2	4	4	0	10	12	4	10	6	2	4
2_x	0	0	0	8	0	4	4	4	0	6	8	6	12	6	4	2
3_x	14	4	2	2	10	6	4	2	6	4	4	0	2	2	2	0
4_x	0	0	0	6	0	10	10	6	0	4	6	4	2	8	6	2
5_x	4	8	6	2	2	4	4	2	0	4	4	0	12	2	4	6
6_x	0	4	2	4	8	2	6	2	8	4	4	2	4	2	0	12
7_x	2	4	10	4	0	4	8	4	2	4	8	2	2	2	4	4
8_x	0	0	0	12	0	8	8	4	0	6	2	8	8	2	2	4
9_x	10	2	4	0	2	4	6	0	2	2	8	0	10	0	2	12
A_x	0	8	6	2	2	8	6	0	6	4	6	0	4	0	2	10
B_x	2	4	0	10	2	2	4	0	2	6	2	6	6	4	2	12
C_x	0	0	0	8	0	6	6	0	0	6	6	4	6	6	14	2
D_x	6	6	4	8	4	8	2	6	0	6	4	6	0	2	0	2
E_x	0	4	8	8	6	6	4	0	6	6	4	0	0	4	0	8
F_x	2	0	2	4	4	6	4	2	4	8	2	2	2	6	8	8
10_x	0	0	0	0	0	0	2	14	0	6	6	12	4	6	8	6
11_x	6	8	2	4	6	4	8	6	4	0	6	6	0	4	0	0
12_x	0	8	4	2	6	6	4	6	6	4	2	6	6	0	4	0
13_x	2	4	4	6	2	0	4	6	2	0	6	8	4	6	4	6
14_x	0	8	8	0	10	0	4	2	8	2	2	4	4	8	4	0
15_x	0	4	6	4	2	2	4	10	6	2	0	10	0	4	6	4
16_x	0	8	10	8	0	2	2	6	10	2	0	2	0	6	2	6
17_x	4	4	6	0	10	6	0	2	4	4	4	6	6	6	2	0
18_x	0	6	6	0	8	4	2	2	2	4	6	8	6	6	2	2
19_x	2	6	2	4	0	8	4	6	10	4	0	4	2	8	4	0
$1A_x$	0	6	4	0	4	6	6	6	6	2	2	0	4	4	6	8
$1B_x$	4	4	2	4	10	6	6	4	6	2	2	4	2	2	4	2
$1C_x$	0	10	10	6	6	0	0	12	6	4	0	0	2	4	4	0
$1D_x$	4	2	4	0	8	0	0	2	10	0	2	6	6	6	14	0
$1E_x$	0	2	6	0	14	2	0	0	6	4	10	8	2	2	6	2
$1F_x$	2	4	10	6	2	2	2	8	6	8	0	0	0	4	6	4
20_x	0	0	0	10	0	12	8	2	0	6	4	4	4	2	0	12
21_x	0	4	2	4	4	8	10	0	4	4	10	0	4	0	2	8
22_x	10	4	6	2	2	8	2	2	2	2	6	0	4	0	4	10
23_x	0	4	4	8	0	2	6	0	6	6	2	10	2	4	0	10
24_x	12	0	0	2	2	2	2	0	14	14	2	0	2	6	2	4
25_x	6	4	4	12	4	4	4	10	2	2	2	0	4	2	2	2
26_x	0	0	4	10	10	10	2	4	0	4	6	4	4	4	2	0
27_x	10	4	2	0	2	4	2	0	4	8	0	4	8	8	4	4
28_x	12	2	2	8	2	6	12	0	0	2	6	0	4	0	6	2
29_x	4	2	2	10	0	2	4	0	0	14	10	2	4	6	0	4
$2A_x$	4	2	4	6	0	2	8	2	2	14	2	6	2	6	2	2
$2B_x$	12	2	2	2	4	6	6	2	0	2	6	2	6	0	8	4
$2C_x$	4	2	2	4	0	2	10	4	2	2	4	8	8	4	2	6
$2D_x$	6	2	6	2	8	4	4	4	2	4	6	0	8	2	0	6
$2E_x$	6	6	2	2	0	2	4	6	4	0	6	2	12	2	6	4
$2F_x$	2	2	2	2	2	6	8	8	2	4	4	6	8	2	4	2
30_x	0	4	6	0	12	6	2	2	8	2	4	4	6	2	2	4
31_x	4	8	2	10	2	2	2	2	6	0	0	2	2	4	10	8
32_x	4	2	6	4	4	2	2	4	6	6	4	8	2	2	8	0
33_x	4	4	6	2	10	8	4	2	4	0	2	2	4	6	2	4
34_x	0	8	16	6	2	0	0	12	6	0	0	0	0	8	0	6
35_x	2	2	4	0	8	0	0	0	14	4	6	8	0	2	14	0
36_x	2	6	2	2	8	0	2	2	4	2	6	8	6	4	10	0
37_x	2	2	12	4	2	4	4	10	4	4	2	6	0	2	2	4
38_x	0	6	2	2	2	0	2	2	4	6	4	4	4	6	10	10
39_x	6	2	2	4	12	6	4	8	4	0	2	4	2	4	4	0
$3A_x$	6	4	6	4	6	8	0	6	2	2	6	2	2	6	4	0
$3B_x$	2	6	4	0	0	2	4	6	4	6	8	6	4	4	6	2
$3C_x$	0	10	4	0	12	0	4	2	6	0	4	12	4	4	2	0
$3D_x$	0	8	6	2	2	6	0	8	4	4	0	4	0	12	4	4
$3E_x$	4	8	2	2	2	4	4	14	4	2	0	2	0	8	4	4
$3F_x$	4	8	4	2	4	0	2	4	4	2	4	8	8	6	2	2

شکل ۵: جدول توزیع Sbox اول

Input XOR	Output XOR															
	0_x	1_x	2_x	3_x	4_x	5_x	6_x	7_x	8_x	9_x	A_x	B_x	C_x	D_x	E_x	F_x
0_x	64	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1_x	0	0	0	4	0	2	6	4	0	14	8	6	8	4	6	2
2_x	0	0	0	2	0	4	6	4	0	0	4	6	10	10	12	6
3_x	4	8	4	8	4	6	4	2	4	2	2	4	6	2	0	4
4_x	0	0	0	0	0	6	0	14	0	6	10	4	10	6	4	4
5_x	2	0	4	8	2	4	6	6	2	0	8	4	2	4	10	2
6_x	0	12	6	4	6	4	6	2	2	10	2	8	2	0	0	0
7_x	4	6	6	4	2	4	4	2	6	4	2	4	4	6	0	6
8_x	0	0	0	4	0	4	0	8	0	10	16	6	6	0	6	4
9_x	14	2	4	10	2	8	2	6	2	4	0	0	2	2	2	4
A_x	0	6	6	2	10	4	10	2	6	2	2	4	2	2	4	2
B_x	6	2	2	0	2	4	6	2	10	2	0	6	6	4	4	8
C_x	0	0	0	4	0	14	0	10	0	6	2	4	4	8	6	6
D_x	6	2	6	2	10	2	0	4	0	10	4	2	8	2	2	4
E_x	0	6	12	8	0	4	2	0	8	2	4	4	6	2	0	6
F_x	0	8	2	0	6	6	8	2	4	4	4	6	8	0	4	2
10_x	0	0	0	8	0	4	10	2	0	2	8	10	0	10	6	4
11_x	6	6	4	6	4	0	6	4	8	2	10	2	2	4	0	0
12_x	0	6	2	6	2	4	12	4	6	4	0	4	4	6	2	2
13_x	4	0	4	0	8	6	6	0	0	2	0	6	4	8	2	14
14_x	0	6	6	4	10	0	2	12	6	2	2	2	4	4	2	2
15_x	6	8	2	0	8	2	0	2	2	2	2	2	2	14	10	2
16_x	0	8	6	4	2	2	4	2	6	4	6	2	6	0	6	6
17_x	6	4	8	6	4	4	0	4	6	2	4	4	4	2	4	2
18_x	0	6	4	6	10	4	0	2	4	8	0	0	4	8	2	6
19_x	2	4	6	4	4	2	4	2	6	4	6	8	0	6	4	2
$1A_x$	0	6	8	4	2	4	2	2	8	2	2	6	2	4	4	8
$1B_x$	0	6	4	4	0	12	6	4	2	2	2	4	4	2	10	2
$1C_x$	0	4	6	6	12	0	4	0	10	2	6	2	0	0	10	2
$1D_x$	0	6	2	2	6	0	4	16	4	4	2	0	0	4	6	8
$1E_x$	0	4	8	2	10	6	6	0	8	4	0	2	4	4	0	6
$1F_x$	4	2	6	6	2	2	2	4	8	6	10	6	4	0	0	2
20_x	0	0	0	2	0	12	10	4	0	0	0	2	14	2	8	10
21_x	0	4	6	8	2	10	4	2	2	6	4	2	6	2	0	6
22_x	4	12	8	4	2	2	0	0	2	8	8	6	0	6	0	2
23_x	8	2	0	2	8	4	2	6	4	8	2	2	6	4	2	4
24_x	10	4	0	0	0	4	0	2	6	8	6	10	8	0	2	4
25_x	6	0	12	2	8	6	10	0	0	8	2	6	0	0	2	2
26_x	2	2	4	4	2	2	10	14	2	0	4	2	2	4	6	4
27_x	6	0	0	2	6	4	2	4	4	4	8	4	8	0	6	6
28_x	8	0	8	2	4	12	2	0	2	6	2	0	6	2	0	10
29_x	0	2	4	10	2	8	6	4	0	10	0	2	10	0	2	4
$2A_x$	4	0	4	8	6	2	4	4	6	6	2	6	2	2	4	4
$2B_x$	2	2	6	4	0	2	2	6	2	8	8	4	4	4	8	2
$2C_x$	10	6	8	6	0	6	4	4	4	2	4	4	0	0	2	4
$2D_x$	2	2	2	4	0	0	0	2	8	4	4	6	10	2	14	4
$2E_x$	2	4	0	2	10	4	2	0	2	2	6	2	8	8	10	2
$2F_x$	12	4	6	8	2	6	2	8	0	4	0	2	0	8	2	0
30_x	0	4	0	2	4	4	8	6	10	6	2	12	0	0	0	6
31_x	0	10	2	0	6	2	10	2	6	0	2	0	6	6	4	8
32_x	8	4	6	0	6	4	4	8	4	6	8	0	2	2	2	0
33_x	2	2	6	10	2	0	0	6	4	4	12	8	4	2	2	0
34_x	0	12	6	4	6	0	4	4	4	0	4	6	4	2	4	4
35_x	0	12	4	6	2	4	4	0	10	0	0	8	0	8	0	6
36_x	8	2	4	0	4	0	4	2	0	8	4	2	6	16	2	2
37_x	6	2	2	2	6	6	4	8	2	2	6	2	2	2	4	8
38_x	0	8	8	10	6	2	2	0	4	0	4	2	4	0	4	10
39_x	0	2	0	0	8	0	10	4	10	0	8	4	4	4	4	6
$3A_x$	4	0	2	8	4	2	2	2	4	8	2	0	4	10	10	2
$3B_x$	16	4	4	2	8	2	2	6	4	4	4	2	0	2	2	2
$3C_x$	0	2	6	2	8	4	6	0	10	2	2	4	4	10	4	0
$3D_x$	0	16	10	2	4	2	4	2	8	0	0	8	0	6	2	0
$3E_x$	4	4	0	10	2	4	2	14	4	2	6	6	0	0	6	0
$3F_x$	4	0	0	2	0	8	2	4	0	2	4	4	4	14	10	6

شکل ۶: جدول توزیع Sbox دوم

Input XOR	Output XOR															
	0_x	1_x	2_x	3_x	4_x	5_x	6_x	7_x	8_x	9_x	A_x	B_x	C_x	D_x	E_x	F_x
0_x	64	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1_x	0	0	0	2	0	4	2	12	0	14	0	4	8	2	6	10
2_x	0	0	0	2	0	2	0	8	0	4	12	10	4	6	8	8
3_x	8	6	10	4	8	6	0	6	4	4	0	0	0	4	2	2
4_x	0	0	0	4	0	2	4	2	0	12	8	4	6	8	10	4
5_x	6	2	4	8	6	10	6	2	2	8	2	0	2	0	4	2
6_x	0	10	6	6	10	0	4	12	2	4	0	0	6	4	0	0
7_x	2	0	0	4	4	4	4	2	10	4	4	8	4	4	4	6
8_x	0	0	0	10	0	4	4	6	0	6	6	6	6	0	8	8
9_x	10	2	0	2	10	4	6	2	0	6	0	4	6	2	4	6
A_x	0	10	6	0	14	6	4	0	4	6	6	0	4	0	2	2
B_x	2	6	2	10	2	2	4	0	4	2	6	0	2	8	14	0
C_x	0	0	0	8	0	12	12	4	0	8	0	4	2	10	2	2
D_x	8	2	8	0	0	4	2	0	2	8	14	2	6	2	4	2
E_x	0	4	4	2	4	2	4	4	10	4	4	4	4	4	2	8
F_x	4	6	4	6	2	2	4	8	6	2	6	2	0	6	2	4
10_x	0	0	0	4	0	12	4	8	0	4	2	6	2	14	0	8
11_x	8	2	2	6	4	0	2	0	8	4	12	2	10	0	2	2
12_x	0	2	8	2	4	8	0	8	8	0	2	2	4	2	14	0
13_x	4	4	12	0	2	2	2	10	2	2	2	2	4	4	4	8
14_x	0	6	4	4	6	4	6	2	8	6	6	2	2	0	0	8
15_x	4	8	2	8	2	4	8	0	4	2	2	2	2	6	8	2
16_x	0	6	10	2	8	4	2	0	2	2	2	8	4	6	4	4
17_x	0	6	6	0	6	2	4	4	6	2	2	10	6	8	2	0
18_x	0	8	4	6	6	0	6	2	4	0	4	2	10	0	6	6
19_x	4	2	4	8	4	2	10	2	2	2	6	8	2	6	0	2
$1A_x$	0	8	6	4	4	0	6	4	4	8	0	10	2	2	2	4
$1B_x$	4	10	2	0	2	4	2	4	8	2	2	8	4	2	8	2
$1C_x$	0	6	8	8	4	2	8	0	12	0	10	0	4	0	2	0
$1D_x$	0	2	0	6	2	8	4	6	2	0	4	2	4	10	0	14
$1E_x$	0	4	8	2	4	6	0	4	10	0	2	6	4	8	4	2
$1F_x$	0	6	8	0	10	6	4	6	4	2	2	10	4	0	0	2
20_x	0	0	0	0	0	4	4	8	0	2	2	4	10	16	12	2
21_x	10	8	8	0	8	4	2	4	0	6	6	6	0	0	2	0
22_x	12	6	4	4	2	4	10	2	0	4	4	2	4	4	0	2
23_x	2	2	0	6	0	2	4	0	4	12	4	2	6	4	8	8
24_x	4	8	2	12	6	4	2	10	2	2	2	4	2	0	4	0
25_x	6	0	2	0	8	2	0	2	8	8	2	2	4	4	10	6
26_x	6	2	0	4	4	0	4	0	4	2	14	0	8	10	0	6
27_x	0	2	4	16	8	6	6	6	0	2	4	4	0	2	2	2
28_x	6	2	10	0	6	4	0	4	4	2	4	8	2	2	8	2
29_x	0	2	8	4	0	4	0	6	4	10	4	8	4	4	4	2
$2A_x$	2	6	0	4	2	4	4	6	4	8	4	4	4	2	4	6
$2B_x$	10	2	6	6	4	4	8	0	4	2	2	0	2	4	4	6
$2C_x$	10	4	6	2	4	2	2	2	4	10	4	4	0	2	6	2
$2D_x$	4	2	4	4	4	2	4	16	2	0	0	4	4	2	6	6
$2E_x$	4	0	2	10	0	6	10	4	2	6	6	2	2	0	2	8
$2F_x$	8	2	0	0	4	4	4	2	6	4	6	2	4	8	4	6
30_x	0	10	8	6	2	0	4	2	10	4	4	6	2	0	6	0
31_x	2	6	2	0	4	2	8	8	2	2	2	0	2	12	6	6
32_x	2	0	4	8	2	8	4	4	8	4	2	8	6	2	0	2
33_x	4	4	6	8	6	6	0	2	2	2	6	4	12	0	0	2
34_x	0	6	2	2	16	2	2	2	12	2	4	0	4	2	0	8
35_x	4	6	0	10	8	0	2	2	6	0	0	6	2	10	2	6
36_x	4	4	4	4	0	6	6	4	4	4	4	4	0	6	2	8
37_x	4	8	2	4	2	2	6	0	2	4	8	4	10	0	6	2
38_x	0	8	12	0	2	2	6	6	2	10	2	2	0	8	0	4
39_x	2	6	4	0	6	4	6	4	8	0	4	4	2	4	8	2
$3A_x$	6	0	2	2	4	6	4	4	4	2	2	6	12	2	6	2
$3B_x$	2	2	6	0	0	10	4	8	4	2	4	8	4	4	0	6
$3C_x$	0	2	4	2	12	2	0	6	2	0	2	8	4	6	4	10
$3D_x$	4	6	8	6	2	2	2	2	10	2	6	6	2	4	2	0
$3E_x$	8	6	4	4	2	10	2	0	2	2	4	2	4	2	10	2
$3F_x$	2	6	4	0	0	10	8	2	2	8	6	4	6	2	0	4

شکل ۷: جدول توزیع Sboxسوم

Input XOR	Output XOR															
	0_x	1_x	2_x	3_x	4_x	5_x	6_x	7_x	8_x	9_x	A_x	B_x	C_x	D_x	E_x	F_x
0_x	64	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1_x	0	0	0	0	0	16	16	0	0	16	16	0	0	0	0	0
2_x	0	0	0	8	0	4	4	8	0	4	4	8	8	8	8	0
3_x	8	6	2	0	2	4	8	2	6	0	4	6	0	6	2	8
4_x	0	0	0	8	0	0	12	4	0	12	0	4	8	4	4	8
5_x	4	2	2	8	2	12	0	2	2	0	12	2	8	2	2	4
6_x	0	8	8	4	8	8	0	0	8	0	8	0	4	0	0	8
7_x	4	2	6	4	6	0	16	6	2	0	0	2	4	2	6	4
8_x	0	0	0	4	0	8	4	8	0	4	8	8	4	8	8	0
9_x	8	4	4	4	4	0	8	4	4	0	0	4	4	4	4	8
A_x	0	6	6	0	6	4	4	6	6	4	4	6	0	6	6	0
B_x	0	12	0	8	0	0	0	0	12	0	0	12	8	12	0	0
C_x	0	0	0	4	0	8	4	8	0	4	8	8	4	8	8	0
D_x	8	4	4	4	4	0	0	4	4	8	0	4	4	4	4	8
E_x	0	6	6	4	6	0	4	6	6	4	0	6	4	6	6	0
F_x	0	6	6	4	6	4	0	6	6	0	4	6	4	6	6	0
10_x	0	0	0	0	0	8	12	4	0	12	8	4	0	4	4	8
11_x	4	2	2	16	2	4	0	2	2	0	4	2	16	2	2	4
12_x	0	0	0	8	0	4	4	8	0	4	4	8	8	8	8	0
13_x	8	2	6	0	6	4	0	6	2	8	4	2	0	2	6	8
14_x	0	8	8	0	8	0	8	0	8	8	0	0	0	0	0	16
15_x	8	4	4	0	4	8	0	4	4	0	8	4	0	4	4	8
16_x	0	8	8	4	8	8	0	0	8	0	8	0	4	0	0	8
17_x	4	6	2	4	2	0	0	2	6	16	0	6	4	6	2	4
18_x	0	8	8	8	8	4	0	0	8	0	4	0	8	0	0	8
19_x	4	4	4	0	4	4	16	4	4	0	4	4	0	4	4	4
$1A_x$	0	6	6	4	6	0	4	6	6	4	0	6	4	6	6	0
$1B_x$	0	6	6	4	6	4	0	6	6	0	4	6	4	6	6	0
$1C_x$	0	8	8	8	8	4	0	0	8	0	4	0	8	0	0	8
$1D_x$	4	4	4	0	4	4	0	4	4	16	4	4	0	4	4	4
$1E_x$	0	6	6	0	6	4	4	6	6	4	4	6	0	6	6	0
$1F_x$	0	0	12	8	12	0	0	12	0	0	0	0	8	0	12	0
20_x	0	0	0	8	0	0	0	12	0	0	0	12	8	12	12	0
21_x	0	4	8	0	8	4	8	8	4	0	4	4	0	4	8	0
22_x	8	2	2	0	2	4	8	6	2	8	4	6	0	6	6	0
23_x	4	6	2	8	2	4	0	2	6	0	4	6	8	6	2	4
24_x	0	6	6	4	6	4	0	6	6	0	4	6	4	6	6	0
25_x	0	8	4	4	4	0	0	4	8	8	0	8	4	8	4	0
26_x	0	6	6	0	6	4	8	2	6	8	4	2	0	2	2	8
27_x	4	6	2	8	2	4	0	2	6	0	4	6	8	6	2	4
28_x	16	4	4	0	4	4	4	4	4	4	4	4	0	4	4	0
29_x	0	6	2	8	2	4	0	2	6	8	4	6	8	6	2	0
$2A_x$	0	2	2	16	2	4	4	2	2	4	4	2	16	2	2	0
$2B_x$	8	0	4	0	4	8	16	4	0	0	8	0	0	0	4	8
$2C_x$	8	4	4	4	4	0	8	4	4	8	0	4	4	4	4	0
$2D_x$	4	2	6	4	6	8	0	6	2	0	8	2	4	2	6	4
$2E_x$	16	0	0	0	0	16	0	0	0	0	16	0	0	0	0	16
$2F_x$	16	0	0	0	0	0	16	0	0	16	0	0	0	0	0	16
30_x	0	6	6	4	6	4	0	6	6	0	4	6	4	6	6	0
31_x	0	8	4	4	4	0	0	4	8	8	0	8	4	8	4	0
32_x	16	6	6	4	6	0	4	2	6	4	0	2	4	2	2	0
33_x	0	2	6	4	6	8	8	6	2	0	8	2	4	2	6	0
34_x	0	12	12	8	12	0	0	0	12	0	0	0	8	0	0	0
35_x	0	4	8	0	8	4	8	8	4	0	4	4	0	4	8	0
36_x	0	2	2	4	2	0	4	6	2	4	0	6	4	6	6	16
37_x	0	2	6	4	6	8	8	6	2	0	8	2	4	2	6	0
38_x	0	4	4	0	4	4	4	4	4	4	4	4	0	4	4	16
39_x	0	6	2	8	2	4	0	2	6	8	4	6	8	6	2	0
$3A_x$	0	4	4	0	4	8	8	4	4	8	8	4	0	4	4	0
$3B_x$	16	4	4	0	4	0	0	4	4	0	0	4	0	4	4	16
$3C_x$	0	4	4	4	4	0	8	4	4	8	0	4	4	4	4	8
$3D_x$	4	2	6	4	6	8	0	6	2	0	8	2	4	2	6	4
$3E_x$	0	2	2	8	2	12	4	2	2	4	12	2	8	2	2	0
$3F_x$	8	4	0	8	0	0	0	0	4	16	0	4	8	4	0	8

شکل ۸: جدول توزیع Sbox چهارم

Input XOR	Output XOR															
	0_x	1_x	2_x	3_x	4_x	5_x	6_x	7_x	8_x	9_x	A_x	B_x	C_x	D_x	E_x	F_x
0_x	64	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1_x	0	0	0	4	0	10	8	6	0	4	2	2	12	10	2	4
2_x	0	0	0	4	0	10	6	4	0	6	4	2	4	8	10	6
3_x	8	2	4	6	4	4	2	2	6	8	6	4	4	0	2	2
4_x	0	0	0	8	0	4	10	6	0	6	6	4	8	6	0	6
5_x	12	2	0	4	0	4	8	2	4	0	16	2	0	2	0	8
6_x	0	8	4	6	4	6	2	2	4	4	6	0	6	0	2	10
7_x	2	0	4	8	4	2	6	6	2	8	6	2	2	0	6	6
8_x	0	0	0	2	0	8	10	4	0	4	10	4	8	4	4	6
9_x	8	6	0	4	0	6	6	2	2	10	2	8	6	2	0	2
A_x	0	6	8	6	0	8	0	0	8	10	4	2	8	0	0	4
B_x	4	2	2	4	8	10	6	4	2	6	2	2	6	2	2	2
C_x	0	0	0	10	0	2	10	2	0	6	10	6	6	6	2	4
D_x	10	4	2	2	0	6	16	0	0	2	10	2	2	4	0	4
E_x	0	6	4	8	4	6	10	2	4	4	4	2	4	0	2	4
F_x	4	4	0	8	0	2	0	2	8	2	4	2	8	4	4	12
10_x	0	0	0	0	0	4	4	12	0	2	8	10	4	6	12	2
11_x	6	6	10	10	4	0	2	6	2	4	0	6	2	4	2	0
12_x	0	2	4	2	10	4	0	10	8	6	0	6	0	6	6	0
13_x	0	0	6	2	8	0	0	4	4	6	2	8	2	8	10	4
14_x	0	12	2	6	4	0	4	4	8	4	4	4	6	2	4	0
15_x	4	8	0	2	8	0	2	4	2	2	4	2	4	8	8	6
16_x	0	6	10	2	14	0	2	2	4	4	0	6	0	4	6	4
17_x	0	6	8	4	8	4	0	2	8	4	0	2	2	8	6	2
18_x	0	10	8	0	6	4	0	4	4	4	6	4	4	4	0	6
19_x	0	4	6	2	4	4	2	6	4	2	2	4	12	2	10	0
$1A_x$	0	2	16	2	12	2	0	6	4	0	0	4	0	4	4	8
$1B_x$	2	8	12	0	0	2	2	6	8	4	0	6	0	0	8	6
$1C_x$	0	10	2	6	6	6	6	4	8	2	0	4	4	4	2	0
$1D_x$	4	6	2	0	8	2	4	6	6	0	8	6	2	4	2	4
$1E_x$	0	2	6	2	4	0	0	2	12	2	2	6	2	10	10	4
$1F_x$	0	6	8	4	8	8	0	6	6	2	0	6	0	6	2	2
20_x	0	0	0	8	0	8	2	6	0	4	4	4	6	6	8	8
21_x	0	0	0	6	6	2	6	4	6	10	14	4	0	0	4	2
22_x	14	4	0	10	0	2	12	2	2	2	10	2	0	0	2	2
23_x	2	0	0	4	2	2	10	4	0	8	8	2	6	8	0	8
24_x	6	2	8	4	4	4	6	2	2	6	6	2	6	2	2	2
25_x	6	0	0	8	2	8	2	6	6	4	2	2	4	2	6	6
26_x	12	0	0	4	0	4	4	4	0	8	4	0	12	8	0	4
27_x	12	2	0	2	0	12	2	2	4	4	8	4	8	2	2	0
28_x	2	8	4	6	2	4	6	0	6	6	4	0	2	2	2	10
29_x	6	4	6	8	8	4	6	2	0	0	2	2	10	0	2	4
$2A_x$	4	4	0	2	2	4	6	2	0	0	6	4	10	4	4	12
$2B_x$	4	6	2	6	0	0	12	2	0	4	12	2	6	4	0	4
$2C_x$	8	6	2	6	4	8	6	0	4	4	0	2	6	0	6	2
$2D_x$	4	4	0	4	0	6	4	2	4	12	0	4	4	6	4	6
$2E_x$	6	0	2	4	0	6	6	4	2	10	6	10	6	2	0	0
$2F_x$	10	4	0	2	2	6	10	2	0	2	2	4	6	2	2	10
30_x	0	4	8	4	6	4	0	6	10	4	2	4	2	6	4	0
31_x	0	6	6	4	10	2	0	0	4	4	0	0	4	6	12	6
32_x	4	6	0	2	6	4	6	0	6	0	4	6	4	10	6	0
33_x	8	10	0	14	8	0	0	8	2	0	2	4	0	4	4	0
34_x	0	4	4	2	14	4	0	8	6	8	2	2	0	4	6	0
35_x	0	4	16	0	8	4	0	4	4	4	0	8	0	4	4	4
36_x	4	4	4	6	2	2	2	12	2	4	4	8	2	4	4	0
37_x	4	2	2	2	4	2	0	8	2	2	2	12	6	2	8	6
38_x	0	4	8	4	12	0	0	8	10	2	0	0	0	4	2	10
39_x	0	8	12	0	2	2	2	2	12	4	0	8	0	4	4	4
$3A_x$	0	14	4	0	4	6	0	0	6	2	10	8	0	0	4	6
$3B_x$	0	2	2	2	4	4	8	6	8	2	2	2	6	14	2	0
$3C_x$	0	0	10	2	6	0	0	2	6	2	2	10	2	4	10	8
$3D_x$	0	6	12	2	4	8	0	8	8	2	2	0	2	2	4	4
$3E_x$	4	4	10	0	2	4	8	8	2	2	0	2	6	8	4	0
$3F_x$	8	6	6	0	4	2	2	4	4	2	8	6	2	4	6	0

شکل ۹: جدول توزیع Sboxپنجم

Input XOR	Output XOR															
	0_x	1_x	2_x	3_x	4_x	5_x	6_x	7_x	8_x	9_x	A_x	B_x	C_x	D_x	E_x	F_x
0_x	64	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1_x	0	0	0	6	0	2	6	2	0	4	2	4	6	16	14	2
2_x	0	0	0	2	0	10	6	10	0	2	4	8	6	6	8	2
3_x	0	8	0	8	0	6	4	6	4	4	4	12	2	4	2	0
4_x	0	0	0	8	0	0	8	0	0	6	8	10	2	4	10	8
5_x	10	2	4	4	4	8	8	4	2	2	0	4	0	8	0	4
6_x	0	8	4	4	8	4	2	2	12	0	2	6	6	2	2	2
7_x	6	6	4	0	2	10	2	2	2	2	6	6	8	0	6	2
8_x	0	0	0	6	0	2	16	4	0	2	6	2	4	12	6	4
9_x	10	4	2	6	0	2	6	2	4	0	8	6	4	4	2	4
A_x	0	14	4	4	0	2	2	2	10	4	4	4	6	4	2	2
B_x	4	6	2	0	2	2	12	8	2	2	2	6	8	2	0	6
C_x	0	0	0	12	0	10	4	6	0	8	4	4	2	12	2	0
D_x	12	0	2	10	6	4	4	2	4	2	6	0	2	6	0	4
E_x	0	6	4	0	4	4	10	8	6	2	4	6	2	0	6	2
F_x	2	2	2	2	6	2	6	2	10	4	8	2	6	4	4	2
10_x	0	0	0	8	0	8	0	12	0	4	2	6	8	4	6	6
11_x	6	2	6	4	6	2	6	4	6	6	4	2	4	0	6	0
12_x	0	8	4	2	0	4	2	0	4	10	6	2	8	6	4	4
13_x	6	6	12	0	12	2	0	6	6	2	0	4	0	2	4	2
14_x	0	4	6	2	8	6	0	2	6	10	4	0	2	4	6	4
15_x	2	2	6	6	4	4	2	6	2	6	8	4	4	0	4	4
16_x	0	4	14	6	8	4	2	6	2	0	2	0	4	2	0	10
17_x	2	6	8	0	0	2	0	2	2	6	0	8	8	2	12	6
18_x	0	4	6	6	8	4	2	2	6	4	6	4	2	4	2	4
19_x	2	6	0	2	4	4	4	6	4	8	6	4	2	2	6	4
$1A_x$	0	6	6	0	8	2	4	6	4	2	4	6	2	0	4	10
$1B_x$	0	4	10	2	4	4	2	6	6	6	2	2	6	6	2	2
$1C_x$	0	0	8	2	12	2	6	2	8	6	6	2	4	0	4	2
$1D_x$	2	4	0	6	8	6	0	2	6	8	6	0	2	4	0	10
$1E_x$	0	10	8	2	8	2	0	2	6	4	2	4	6	4	2	4
$1F_x$	0	6	6	8	6	4	2	4	4	2	2	0	2	4	2	12
20_x	0	0	0	0	0	6	6	4	0	4	8	8	4	6	10	8
21_x	2	8	6	8	4	4	6	6	8	4	0	4	0	2	2	0
22_x	16	2	4	6	2	4	2	0	6	4	8	2	0	2	2	4
23_x	0	4	0	4	4	6	10	4	2	2	6	2	4	6	6	4
24_x	10	8	0	6	12	6	10	4	8	0	0	0	0	0	0	0
25_x	0	2	4	2	0	4	4	0	4	0	10	10	4	10	6	4
26_x	2	2	0	12	2	2	6	2	4	4	8	0	6	6	8	0
27_x	8	4	0	8	2	4	2	4	0	6	2	4	4	8	2	6
28_x	6	8	4	6	0	4	2	2	4	8	2	6	4	2	2	4
29_x	2	4	4	0	8	8	6	8	6	4	0	4	4	4	2	0
$2A_x$	6	0	0	6	6	4	6	8	2	4	0	2	2	4	6	8
$2B_x$	12	0	4	0	0	4	2	2	2	6	10	6	10	2	4	0
$2C_x$	4	2	6	0	0	6	8	6	4	2	2	8	4	6	4	2
$2D_x$	6	2	2	6	6	4	4	2	6	2	4	8	4	2	4	2
$2E_x$	4	6	2	4	2	4	4	2	4	2	4	6	4	10	4	2
$2F_x$	10	0	4	8	0	6	6	2	0	4	4	2	6	2	2	8
30_x	0	12	8	2	0	6	0	0	6	6	0	2	8	2	6	6
31_x	2	6	10	4	2	2	2	4	6	0	2	6	0	2	4	12
32_x	4	2	2	8	10	8	8	6	0	2	2	4	4	2	2	0
33_x	4	2	2	2	6	0	4	0	10	6	6	4	0	4	8	6
34_x	0	4	4	2	6	4	0	4	6	2	6	4	2	8	0	12
35_x	6	12	4	2	4	2	2	4	8	2	2	0	6	4	4	2
36_x	0	2	2	4	4	4	4	0	2	10	12	4	0	10	4	2
37_x	10	2	2	6	14	2	2	6	2	0	4	6	2	0	4	2
38_x	0	4	14	0	8	2	0	4	4	4	2	0	8	2	4	8
39_x	2	4	8	0	6	2	0	6	2	6	4	2	8	6	2	6
$3A_x$	8	4	0	4	6	2	0	4	6	8	6	0	6	0	4	6
$3B_x$	0	4	6	6	2	2	2	14	0	12	0	4	2	2	8	0
$3C_x$	0	6	16	0	2	2	2	8	4	2	0	12	6	2	2	0
$3D_x$	0	6	2	2	2	6	8	2	4	2	6	2	6	2	4	10
$3E_x$	4	2	2	4	4	0	6	10	4	2	4	6	6	2	6	2
$3F_x$	0	4	6	6	4	8	4	0	4	8	4	0	4	8	2	2

شکل ۱۰: جدول توزیع Sboxششم

Input XOR	Output XOR															
	0_x	1_x	2_x	3_x	4_x	5_x	6_x	7_x	8_x	9_x	A_x	B_x	C_x	D_x	E_x	F_x
0_x	64	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1_x	0	0	0	2	0	4	4	14	0	12	4	6	2	6	6	4
2_x	0	0	0	0	0	12	2	2	0	4	0	4	8	12	6	14
3_x	8	2	12	2	6	8	6	0	6	4	4	2	2	0	0	2
4_x	0	0	0	8	0	4	4	8	0	8	8	12	2	6	2	2
5_x	6	0	0	2	8	0	8	4	0	2	6	0	10	6	6	6
6_x	0	2	12	0	8	4	8	2	4	4	4	2	6	0	6	2
7_x	4	6	4	12	0	4	2	0	0	14	2	6	4	0	0	6
8_x	0	0	0	8	0	0	6	10	0	4	12	4	6	6	0	8
9_x	10	8	4	8	6	2	2	0	2	6	8	2	0	6	0	0
A_x	0	10	6	2	12	2	4	0	4	4	6	4	4	0	0	6
B_x	0	2	2	2	4	8	6	4	4	0	4	2	6	4	2	14
C_x	0	0	0	4	0	4	8	4	0	2	6	0	14	12	8	2
D_x	6	6	2	4	2	6	4	6	6	4	8	8	0	2	0	0
E_x	0	12	10	10	0	2	4	2	8	6	4	2	0	0	2	2
F_x	2	0	0	0	6	8	8	0	6	2	4	6	8	0	6	8
10_x	0	0	0	4	0	2	8	6	0	6	4	10	8	4	8	4
11_x	6	10	10	4	4	2	0	4	4	0	2	8	4	2	2	2
12_x	0	0	8	8	2	8	2	8	6	4	2	8	0	0	8	0
13_x	4	4	2	2	8	6	0	2	2	2	0	4	6	8	14	0
14_x	0	8	6	2	8	8	2	6	4	2	0	2	8	6	0	2
15_x	4	4	8	2	4	0	4	10	8	2	4	4	4	2	0	4
16_x	0	6	10	2	2	2	2	4	10	8	2	2	0	4	10	0
17_x	8	2	4	2	6	4	0	6	4	4	2	2	0	4	8	8
18_x	0	16	2	2	6	0	6	0	6	2	8	0	6	0	2	8
19_x	0	8	0	2	4	4	10	4	8	0	6	4	2	6	2	4
$1A_x$	0	2	4	8	12	4	0	6	4	4	0	2	0	6	4	8
$1B_x$	0	6	2	6	4	2	4	4	6	4	8	4	2	0	10	2
$1C_x$	0	8	4	4	2	6	6	6	6	4	6	8	0	2	0	2
$1D_x$	4	4	4	0	0	2	4	2	4	2	2	4	10	10	8	4
$1E_x$	0	0	2	2	12	6	2	0	12	2	2	4	2	6	8	4
$1F_x$	2	2	10	14	2	4	2	4	4	6	0	2	4	8	0	0
20_x	0	0	0	14	0	8	4	2	0	4	2	8	2	6	0	14
21_x	4	2	6	2	12	2	4	0	6	4	10	2	4	2	2	2
22_x	10	6	0	2	4	4	10	0	4	0	12	2	8	0	0	2
23_x	0	6	2	2	2	4	6	10	0	4	8	2	2	6	0	10
24_x	4	2	0	6	8	2	6	0	8	2	2	0	8	2	12	2
25_x	2	0	2	16	2	4	6	4	6	8	2	4	0	6	0	2
26_x	6	10	0	10	0	6	4	4	2	2	4	6	2	4	2	2
27_x	4	0	2	0	2	2	14	0	4	6	6	2	12	2	4	4
28_x	14	4	6	4	4	6	2	0	6	6	2	2	4	0	2	2
29_x	2	2	0	2	0	8	4	2	4	6	4	4	6	4	12	4
$2A_x$	2	4	0	0	0	2	8	12	0	8	2	4	8	4	4	6
$2B_x$	16	6	2	4	6	10	2	2	2	2	2	2	4	2	2	0
$2C_x$	2	6	6	8	2	2	0	6	0	8	4	2	2	6	8	2
$2D_x$	6	2	4	2	8	8	2	8	2	4	4	0	2	0	8	4
$2E_x$	2	4	8	0	2	2	2	4	0	2	8	4	14	6	0	6
$2F_x$	2	2	2	8	0	2	2	6	4	6	8	8	6	2	0	6
30_x	0	6	8	2	8	4	4	0	10	4	4	6	0	0	2	6
31_x	0	8	4	0	6	2	2	6	6	0	0	2	6	4	8	10
32_x	2	4	0	0	6	4	10	6	6	4	6	2	4	6	2	2
33_x	0	16	6	8	2	0	2	2	4	2	8	4	0	4	6	0
34_x	0	4	14	8	2	2	2	4	16	2	2	2	0	2	0	4
35_x	0	6	0	0	10	8	2	2	6	0	0	8	6	4	4	8
36_x	2	0	2	2	4	6	4	4	2	2	4	2	4	16	10	0
37_x	6	6	6	8	4	2	4	4	4	0	6	8	2	4	0	0
38_x	0	2	2	2	8	8	0	2	2	2	0	6	6	4	10	10
39_x	4	4	16	8	0	6	4	2	4	4	2	6	0	2	2	0
$3A_x$	16	6	4	0	2	0	2	6	0	4	8	10	0	0	4	2
$3B_x$	2	0	0	2	0	4	4	4	2	6	2	6	6	12	12	2
$3C_x$	0	0	8	0	12	8	2	6	6	4	0	2	2	4	6	4
$3D_x$	2	4	12	2	2	2	0	4	6	10	2	6	4	2	0	6
$3E_x$	4	6	6	6	2	0	4	8	2	10	4	6	0	4	2	0
$3F_x$	14	0	0	0	8	0	6	8	4	2	0	0	4	8	4	6

شکل ۱۱: جدول توزیع Sboxهفتم

Input XOR	Output XOR															
	0_x	1_x	2_x	3_x	4_x	5_x	6_x	7_x	8_x	9_x	A_x	B_x	C_x	D_x	E_x	F_x
0_x	64	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1_x	0	0	0	6	0	16	10	0	0	0	6	0	14	6	2	4
2_x	0	0	0	8	0	10	4	2	0	10	2	4	8	8	6	2
3_x	6	0	2	8	2	6	4	0	6	6	6	2	2	0	8	6
4_x	0	0	0	2	0	4	6	12	0	6	8	4	10	4	8	0
5_x	4	10	6	0	0	2	6	0	4	10	4	6	8	2	0	2
6_x	0	0	10	4	6	4	4	8	2	6	4	2	4	2	2	6
7_x	6	2	8	2	8	10	6	6	4	2	0	4	0	0	0	6
8_x	0	0	0	4	0	6	4	2	0	8	6	10	8	2	2	12
9_x	8	4	0	6	0	4	4	6	2	4	6	2	12	2	0	4
A_x	0	0	16	4	6	6	4	0	4	6	4	2	2	0	0	10
B_x	2	8	0	6	2	6	0	4	4	10	0	2	10	2	6	2
C_x	0	0	0	2	0	10	10	6	0	6	6	6	2	6	10	0
D_x	6	0	4	10	2	0	8	6	2	2	6	10	2	2	2	2
E_x	0	0	6	8	4	8	0	2	10	6	2	4	6	2	4	2
F_x	8	0	4	2	2	4	2	2	2	6	4	6	0	2	14	6
10_x	0	0	0	4	0	0	8	12	0	0	8	8	2	10	6	6
11_x	0	6	4	6	2	2	6	6	4	6	4	6	0	4	4	4
12_x	0	4	0	8	6	2	8	4	2	4	4	6	2	4	10	0
13_x	4	2	2	6	8	6	2	2	14	2	2	4	2	2	2	4
14_x	0	16	4	2	6	0	2	6	4	0	4	6	4	6	4	0
15_x	0	10	6	0	6	0	2	8	2	2	0	8	2	6	6	6
16_x	0	12	6	4	6	0	0	0	8	6	6	2	2	6	4	2
17_x	0	6	8	0	6	2	4	6	6	0	2	6	4	4	2	8
18_x	0	12	2	2	8	0	8	0	10	4	4	2	4	2	0	6
19_x	6	4	8	0	8	0	4	2	0	0	12	2	4	6	2	6
$1A_x$	0	4	6	2	8	8	0	4	8	0	0	0	6	2	0	16
$1B_x$	2	4	8	10	2	4	2	8	2	4	8	2	0	2	4	2
$1C_x$	0	12	6	4	6	4	2	2	6	0	4	4	2	10	2	0
$1D_x$	8	6	0	0	10	0	0	8	10	4	2	2	2	8	4	0
$1E_x$	0	4	8	6	8	2	4	4	10	2	2	4	2	0	6	2
$1F_x$	4	2	4	2	6	2	4	0	2	6	2	2	2	16	8	2
20_x	0	0	0	16	0	4	0	0	0	14	6	4	2	0	4	14
21_x	0	0	2	10	2	8	10	0	0	6	6	0	10	2	2	6
22_x	8	0	6	0	6	4	10	2	0	6	8	0	4	4	2	4
23_x	4	8	0	6	0	4	8	6	2	2	10	4	8	0	0	2
24_x	4	0	4	8	4	6	2	4	8	6	2	0	0	4	4	8
25_x	0	4	6	8	2	8	8	0	4	2	4	4	2	2	6	4
26_x	2	6	0	6	4	4	4	6	6	0	4	4	10	4	2	2
27_x	6	6	0	0	2	2	6	2	4	4	6	10	2	6	2	6
28_x	10	2	6	2	4	12	12	0	2	2	4	0	0	0	2	6
29_x	4	0	0	14	2	10	4	2	8	6	4	0	4	2	2	2
$2A_x$	8	8	0	2	0	2	4	0	2	6	8	14	2	8	0	0
$2B_x$	2	2	0	0	4	2	10	4	6	2	4	0	6	4	8	10
$2C_x$	2	6	6	2	4	6	2	0	2	6	4	0	6	4	10	4
$2D_x$	8	0	4	4	6	2	0	0	6	8	2	4	6	4	4	6
$2E_x$	6	2	2	4	2	2	6	12	4	0	4	2	8	8	0	2
$2F_x$	8	12	4	6	6	4	2	2	2	2	4	2	2	4	0	4
30_x	0	4	6	2	10	2	2	2	4	8	0	0	8	4	6	6
31_x	4	6	8	0	4	6	0	4	4	6	10	2	2	4	4	0
32_x	6	6	6	2	4	6	0	2	0	6	8	2	2	6	6	2
33_x	6	6	4	2	4	0	0	10	2	2	0	6	8	4	0	10
34_x	0	2	12	4	10	4	0	4	12	0	2	4	2	2	2	4
35_x	6	4	4	0	10	0	0	4	10	0	0	4	2	8	8	4
36_x	4	6	2	2	2	2	6	8	6	4	2	6	0	4	10	0
37_x	2	2	8	2	4	4	4	2	6	2	0	10	6	10	2	0
38_x	0	4	8	4	2	6	6	2	4	2	2	4	6	4	4	6
39_x	4	4	4	8	0	6	0	6	4	8	2	2	2	4	8	2
$3A_x$	8	8	0	4	2	0	10	4	0	0	0	4	8	6	8	2
$3B_x$	8	2	6	4	4	4	4	0	6	4	4	6	4	4	4	0
$3C_x$	0	6	6	6	6	0	0	8	8	2	4	8	4	2	4	0
$3D_x$	2	2	8	0	10	0	2	12	0	4	0	8	0	2	6	8
$3E_x$	6	4	0	0	4	4	0	10	6	2	6	12	2	4	0	4
$3F_x$	0	6	6	0	4	4	6	10	0	6	8	2	0	4	8	0

شکل ۱۲: جدول توزیع Sboxهشتم