

ADI - 504 adi: Muhammed Ramadan

No: 190290605

1)

$$a) 15 * 29 \bmod 13 \Rightarrow$$
$$435 \bmod 13$$

$$\Rightarrow 435 / 13 = 33, \text{Kalan} = 6$$

$$\Rightarrow \text{Cevap} = 6$$

$$b) -11 * 3 \bmod 13$$

$$\Rightarrow -11 * 3 = -33$$

$$\Rightarrow -33 / 13 = -2, \text{Kalan} = -7$$

Kalan -7 alacağına göre,  $-11 * 3 \bmod 13 = 6$   
cevap = 6

$$c) 1/5 \bmod 13 \Rightarrow$$

$$5^*1 = 5 \bmod 13$$

$$5^*2 = 10 \bmod 13$$

$$5^*3 = 15 \bmod 13$$

$$5^*4 = 20 \bmod 13$$

$$5^*5 = 25 \bmod 13$$

$$5^*6 = 30 \bmod 13$$

$$5^*7 = 35 \bmod 13$$

$$5^*8 = 40 \bmod 13$$

$$\Rightarrow 5^*9 = 45 \bmod 13$$

$$5^*10 = 50 \bmod 13$$

$$5^*11 = 55 \bmod 13$$

$$5^*12 = 60 \bmod 13$$

$$\Rightarrow 5^*8 = 40 \bmod 13 = 3 \bmod 13$$

$$1^*8 \bmod 13 = 8$$
$$\underline{\underline{=}}$$

ADI - SOYADI: Muhammed Ramadan

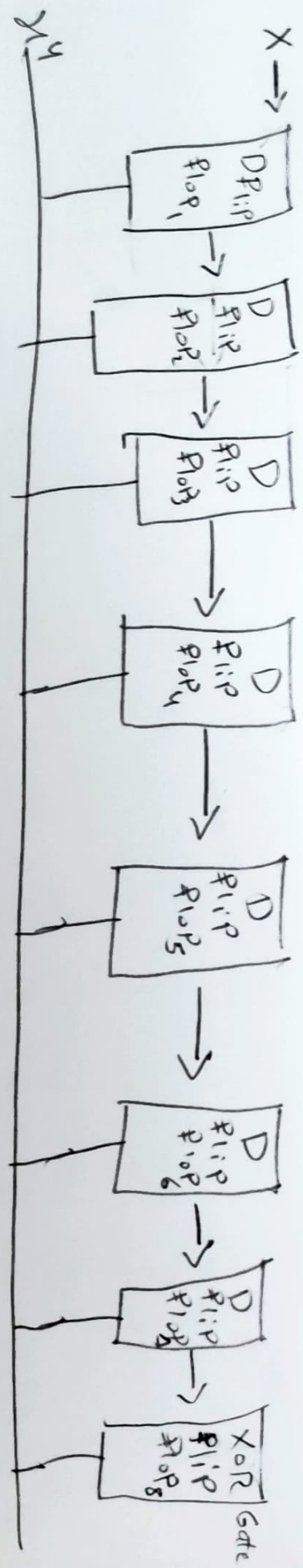
NO: 190290605

2) IFYF xjhzwngd nx ymü uwthjxx tk xfkjLZFwinski  
inlnyfq nsktwrfynts ymw+Zlmtzy nyx js ynwj  
9nkj hdhqj yt uwtyjh y ny kwtr htwrzu ynt  
, ymjky, tw zsfymtwneji Phhjxx

ADI - Soyadı: Muhammed Ramadan  
No: 190290605

3)

a-



ADL SoyaDi: Muhammed Ramadan  
No: 190 290 605

3)

b.

	A	B	C	D	E	F	G	H
0	1	1	1	1	1	1	1	1
1	1	1	1	1	1	1	1	0
2	0	1	1	1	1	1	1	1
3	1	0	1	1	1	1	1	1
4	1	1	0	1	1	1	1	1
5	1	1	1	0	1	1	1	1
6	1	1	1	1	0	1	1	1
7	1	1	1	1	1	0	1	1
8	1	1	1	1	1	1	0	1



ADI-Soyadı: Muhammed Ramadan  
No: 190290605

4)

F-Fonksiyonu

- DES'in ana işlemleri
- F-Fonksiyonu girişleri:

$R_{i-1}$  ve round anahtarı  $K_i$

• 4 Adımları:

- 1- Genişletilmiş E
- 2- Round anahtarı ile XOR
- 3- S-box Substitution
- 4- Permutasyon

