ADI - SOYADI: Muhammed Ramadan

No: 190290605

1)

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

$435 \bmod 13$

$\Rightarrow 435/13 = 33$, Kalan $= 6$

$\Rightarrow$ cevap $= 6$

b) $-11 * 3 \bmod 13$

$\Rightarrow -11 * 3 = -33$

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

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

cevap $= 6$

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

$5 * 1 = 5 \pmod{13}$

$5 * 2 = 10 \pmod{13}$

$5 * 3 = 15 \pmod{13}$

$5 * 4 = 20 \pmod{13}$

$5 * 5 = 25 \pmod{13}$

$5 * 6 = 30 \pmod{13}$

$5 * 7 = 35 \pmod{13}$

$5 * 8 = 40 \pmod{13}$

$\Rightarrow 5 * 9 = 45 \pmod{13}$

$5 * 10 = 50 \pmod{13}$

$5 * 11 = 55 \pmod{13}$

$5 * 12 = 60 \pmod{13}$

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

$1 * 8 \bmod 13 = 8$

ADI - SOYADI: Muhammed Ramadan

NO: 190290605

2)

IfYf xjhzwnyd nx Ymj uwthjxx tk xFkjLZFwinsl

imlnyfq nsktwrfynts Ymwtzlmtzy nyx js Ynwj

9nkj hdhqj yt uwtyjhy ny Kwtr htwwzuyn-

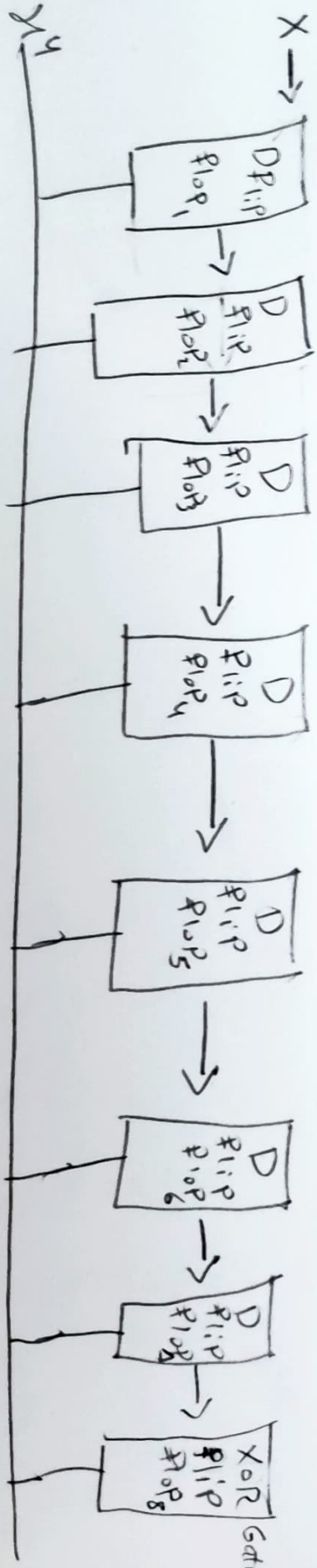
, Ymjky, tw zsFymtwneji Fhhjxx

ADI-Soyadi: Muhammed Ramazan

No: 19029605

3)

a-



ADL_SOYADI: Muhammed Ramadan

ADL SOYADI: Muhammed Ramadan
No: 190290605

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-SOYADI: Muhammed Ramadan

No: 19029605

4)

f-Fonksiyonu

- DES'in ana işlemleri
- f-Fonksiyonu girişler:

R_{i-1} ve round anahtar K_i

- 4 Adımlar:

1- Genişletilmiş E

2- Round anahtarı ile XOR

3- S-box subtitution

4- Permütasyon