F.Ü. Mühendislik Fakültesi

Bilgisayar Mühendisliği Bölümü

Bilgisayar Sistemleri Laboratuvarı

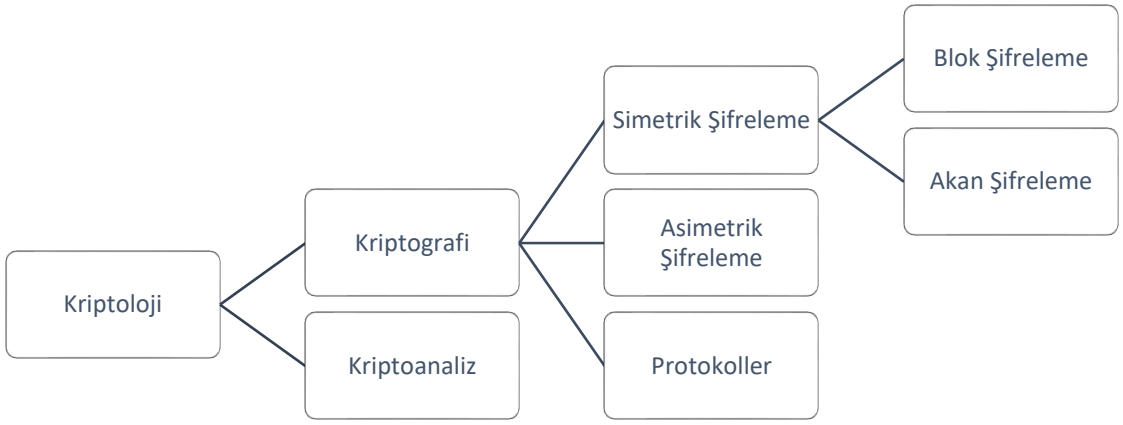
DENEY NO : 3

DENEY ADI : ŞİFRELEME YÖNTEMLERİ

Deneyin amacı:

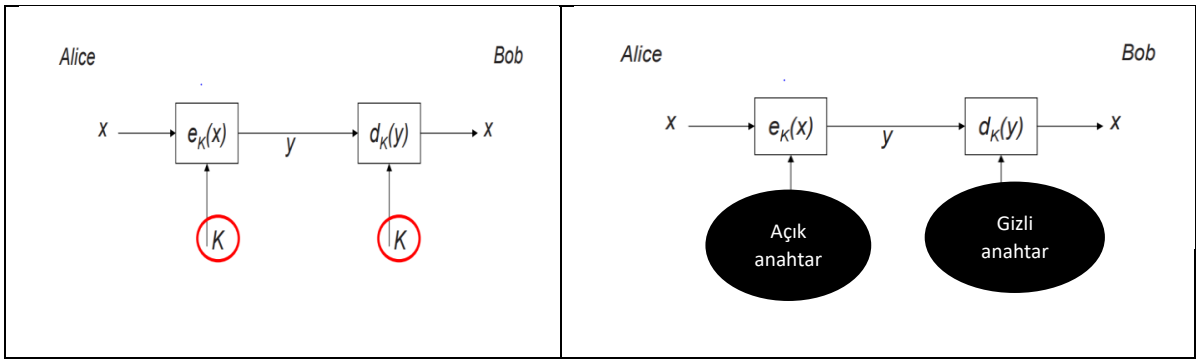
Kriptoloji, kriptografi, kriptoanaliz kavramlarının öğrenilmesi, simetrik şifreleme algoritmalarından DES ve asimetrik şifreleme algoritmalarında RSA algoritmalarının öğrenilmesidir.

Kriptoloji Bilimi



Şekil 1.Kriptoloji bilimi [1]

- Kriptoloji: Haberleşmede veri güvenliğini sağlayan şifreleme cihazlarını, bu cihazlarda kullanılan algoritmaların tasarımını ve bu algoritmaların güvenilirliğini araştırır.
- Kriptografi: iletilen bilginin istenmeyen şahıslar tarafından anlaşılmayacak bir biçime dönüştürülmesinde kullanılan tekniklerin bütünüdür. Güvenliği sağlayan protokolün ortaya konulmasıdır.
- Kriptoanaliz: Kriptolojinin, kriptografik sistemlerin şifrelenmiş metinlerini çözebilmek için bu sistemlerin güvenliklerini inceleyen - zayıf yanlarını bulmaya çalışan dalıdır.



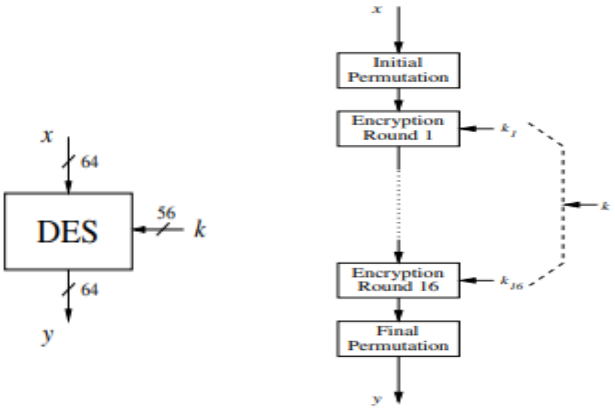
Şekil 2. Simetrik ve asimetrik şifreleme mekanizması [1]

DES Algoritması

Simetrik blok şifreleme algoritması olan DES 1997'de resmi olarak bilgi şifreleme standartı olarak kabul edilmiştir. Ancak 2000 yılında yerini AES'e bırakmıştır. DES algoritması 64 bitlik blok şifreleme algoritmasıdır. Anahtar uzayı ise 56 bit uzunlundadır. Anahtar uzayının 56 bit olması bu algoritmanın güvenli olarak nitelendirmemesine neden olmaktadır. Bu nedenle DES'in güvenilirliğini artırmak için 3DES yöntemi geliştirilmiştir. Bu yöntemde, şifrelenen veri farklı anahtar(lar) ile tekrar geri çözülür ve DES şifrelemesi 3 sefer ardarda yapılır [1].

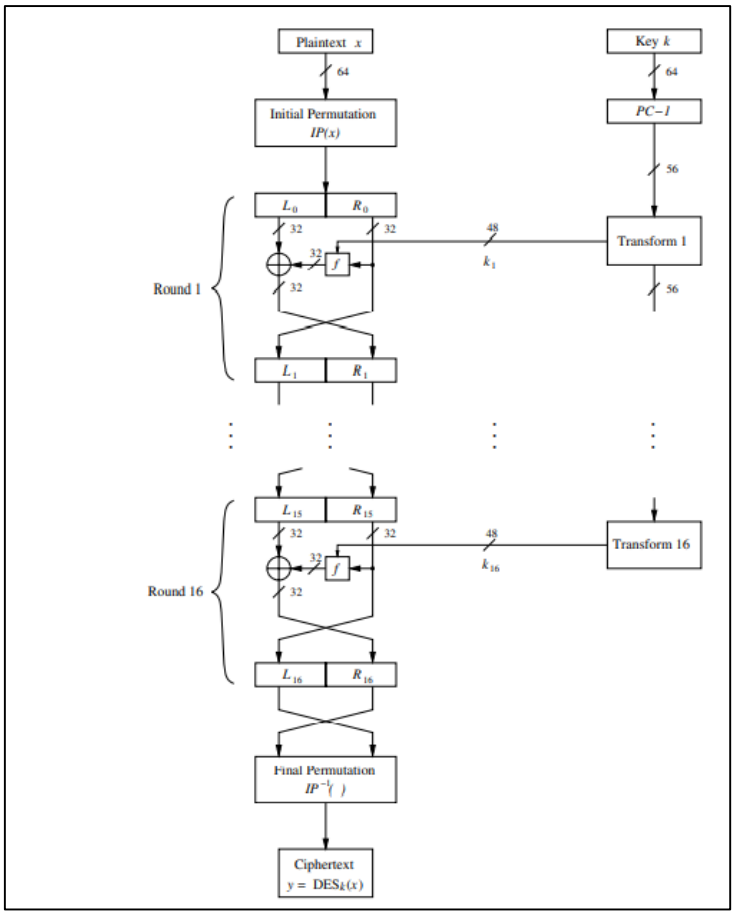
$$y = DES_{k_3}(DES_{k_2}(DES_{k_1}(x)))$$

DES algoritması simetrik şifreleme algoritması olması bakımından hem şifreleme hem de şifre çözme aşamasında aynı anahtarı kullanmaktadır. Şekil 3'de simetrik şifreme yaklaşımı gösterilmiştir. DES 16 adımda veriyi şifrelemektedir. Her bir adımda farklı anahtar kullanmaktadır [1].



- Veri blokları 64 bittir.
- Anahtar uzunluğu 56 bittir.
- Simetrik şifreleme: şifreleme ve şifre çözme sürecinde aynı anahtarı kullanır.
- Her bir adımda yeni anahtar kullanılır.

Şekil 3. DES algoritmasın genel yapısı [1]



Şekil 4. DES Algoritması [1]

$$L_i = R_{i-1},$$
$$R_i = L_{i-1} \oplus f(R_{i-1}, k_i)$$

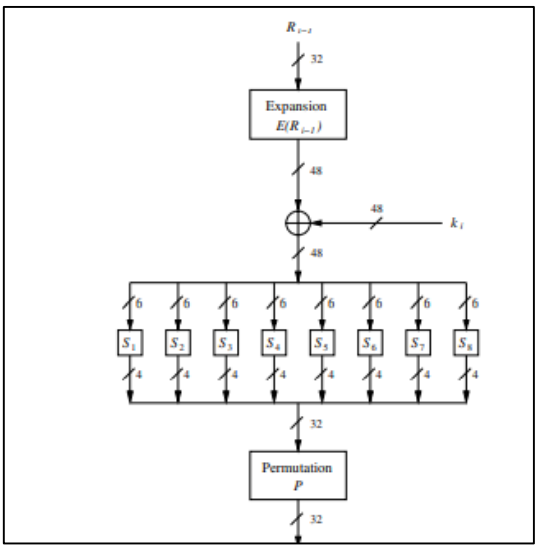
Başlangıç ve bitiş permütasyonları: Şekil 5'de başlangıç permütasyonu (IP) ve bitiş permütasyonu (IP^{-1})gösterilmektedir. Bu permütasyonları kullanmadaki amaç, başlangıçta verilen 64 bitlik veri bloğunu karıştırmaktır. Örneğin, ilk baştaki veri bloğundaki 2 bitin yerine 8 biti koyulmuştur. IP^{-1}'de ise bu işlemlerin tersi yapılmaktadır.

IP							
58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

IP^{-1}							
40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25

Şekil 5. Başlangıç ve bitiş permütasyonları [1]

F fonksiyonu Giriş olarak R_{i-1} ve K_i alır ve dört adımdan oluşan işleme tabi tutar bunlar E'nin genişletilmesi, tura ait anahtar ile XOR'lama, S-BOX yer değiştirme ve permütasyondur.



Şekil 6. F fonksiyonunun blok diyagramı [1]

S-Box'lar 4 satır 16 sütündan oluşan matrislerdir. S-box veriyi 6 bitten 4 bite indirgeme yapılmaktadır. Bunun için sayının ilk ve son biti satır sayısını, ortadaki biti ise sütün sayısını gösterecek şekilde tablodaki sayı alınır. Örneğin sayı, 6 bitlik 100101 olsun, MSB ve LSB biti 11 S-Box daki satır sayısını, ortadaki 0010 ise sütündaki sayısı ifade eder. Böylece yeni 4 bitlik sayı 08'dir.

S_1	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	14	04	13	01	02	15	11	08	03	10	06	12	05	09	00	07
1	00	15	07	04	14	02	13	01	10	06	12	11	09	05	03	08
2	04	01	14	08	13	06	02	11	15	12	09	07	03	10	05	00
3	15	12	08	02	04	09	01	07	05	11	03	14	10	00	06	13

Permütasyon aşamasında ise, 32 bitten oluşan veri, permütasyon tablosundan yararlanılarak karıştırma yapılmaktadır.

RSA Algoritması

- Ron Rivest, Adi Shamir ve Leonard Adleman tarafından 1978'de geliştirilmiştir.
- Yaygın kullanılan asimetrik şifreleme algoritmasıdır.
- RSA algoritması, anahtarın taşınması ve dijital imza olmak üzere iki amaç için kullanılır.
- Açık anahtar (n,e) ile mesaj şifrelenir. Alıcı tarafta gizli anahtarla (d) şifre çözülür.

$$y = e_{k_{pub}}(x) \equiv x^e \bmod n$$

$$x = d_{k_{pr}}(y) \equiv y^d \bmod n$$

Anahtar üretimi

Açık anahtar:$k_{pub} = (n, e)$ gizli anahtar: k_{pr}=d

1. İki asal sayı seç p,q
2. n=p*q
3. Φ(n)=(p-1)*(q-1)
4. GCD(e,Φ(n))=1 olacak şekilde e asal sayısının seçimi
5. d*e≡1 mod Φ(n)
6. return $k_{pub} = (n, e)$ gizli anahtar: k_{pr}=d

Örnek:

A	B
Mesaj x = 4	1. p = 3 ve q = 11 2. n = p · q = 33 3. Φ(n)=(3−1)(11−1) = 20 4. e = 3 5. d ≡ e^{-1} ≡ 7 mod 20
	$k_{pub} = (33,3)$ ←
$y = x^e \equiv 4^3 \equiv 31 \bmod 33$	
	y =31 ⇒
	$y^d = 31^7 \equiv 4 = x \bmod 33$

Kaynaklar

1. Paar, C., & Pelzl, J. (2009). *Understanding cryptography: a textbook for students and practitioners*. Springer Science & Business Media.
2. Heys, H. M. (2002). A tutorial on linear and differential cryptanalysis. *Cryptologia*, *26*(3), 189-221.