BİL 470
KRİPTOGRAFİ
ve
BİLGİSAYAR GÜVENLİĞİ

RAPOR

08.01.2021

Ebru KARDAŞ
141044049

PROGRAMLAMA PROJESİ

C veya Python ile gerçekleştirilecek olan bu araçta şifreleme/deşifreleme ve özüt alma, dosya bütünlüğünün denetimi yöntemleri bizzat gerçeklenecek olup, arşiv/API kullanılmayacaktır. Gerçeklenen programların kaynak kodları açıklamalı olarak verilecektir;

a. AES şifreleme algoritmasının gerçeklenmesi ve şifreleme/deşifrelemede kullanılması (test verileri ile birlikte).
b. Gerçeklenen simetrik şifreleme algoritması kullanılarak CBC ve OFB modlarında çalışmayı gerçekleyip testlerini yapacak şekle getiriniz.
c. Herhangi bir doküman (.doc/.docx, .pdf, ppt, xls vs) üzerinde değişiklik yapılıp yapılmadığını ve yapanın kimliğini anlamak için, özütünü alacak ve sadece işlem yapan kişinin bildiği bir anahtar ile şifreleyip dosyanın sonuna ekleyecek bir araç (b şıkkındaki gerçeklemeyi özüt fonksiyonu olarak kullanınız)
d. Dosyanın bütünlüğünün değişip değişmediğinin kontrolü için, c)deki işlemleri yaparak ilk üretilen özüt değer ile karşılaştıran doğrulama aracını gerçekleyerek örnek testleri gösteriniz.

Ödev problemlerinde yapılan çalışma sonuçları yazılı rapor halinde .doc/docx olarak verilen bitirme zamanından önce Teams'teki ders grubuna yüklenecektir.

AES şifreleme ve algoritması:

Anahtara göre farklı sayıda döngüsel işlem yapılır. Her döngüden sonra anahtar yenilenerek veriye uygulanır. Bunun anlamı tur sayısı kadar anahtar üretimi gerçekleştirilmiş olur. Tur sayısı ise anahtar uzunluğuna bağlıdır.

Şifreleme ve deşifreleme işlemlerinde aynı anahtar kullanılır.

Veri bayt dizileri şeklinde ifade edilir.
128 bit uzunluğundaki veri, 4x4'luk matrislere bölünür. Bu matrislere durum (state) matrisi denir. Matrisin her elemanı 8 bit (1 byte), her satir veya sütun 32 bittir. Her satıra kelime (word) denir. Anahtar da durum matrisine çevrilir. Şifreleme başlangıcında şifresiz metnin durum matrisi ile anahtarın durum matrisi toplanır.

Veri Blogu	**Kelime Uzunluğu**	**Tur Sayısı**
AES-128	4	10
AES-192	6	12
AES-256	8	14

Matris eleman sayısı n olsun:
Anahtar uzunluğu 128 olsun. 0<n<16
Anahtar uzunluğu 192 olsun. 0<n<24
Anahtar uzunluğu 256 olsun. 0<n<32

Bayt değerleri = {b7, b6, b5, b4, b3, b2, b1, b0}

b7x^7 + b6x^6 + b5x^5 + b4x^4 + b3x^3 + b2x^2 + b1x + b0 = Toplam ((i=0 -> 7) bix^i)
Onaltılık tabanda gösterilebilir. (10:A 11:B 12:C 13:D 14:E 15:F)

Veri: 19 A0 9A E9 3D F4 C6 F8 E3 E2 8D 48 B3 2B 2A 08

Durum Matrisi:
19 3D E3 B3
A0 F4 E2 2B
9A C6 8D 2A
E9 F8 48 08 (Örnektir.)

Döngü Yapısı

1. Bayt Değiştirme (SubBytes)
   - Tek doğrusal olmayan işlem
   - İlk işlem
   - Değişiklik S-kutusuna bağlı
   - S-kutusu, durum matrisinin elemanları onaltılık tabanda olduğu için S-kutusu da 16x16 onaltılık tabanda bir matristir.
   - Bu işlem tüm matrise uygulanır.
2. Satir Kaydırma (ShiftRows)
   - Her satir, satir sayısının 1 eksiği kadar elemanı bastan çıkarıp sona ekler.
3. Sütun Karıştırma (MixColumns): Son döngüde yok
   - a(x) = {03}x^3 + {01}x^2 + {01}x + {02}
   - İşlem her sütuna yapılır
4. Tur Anahtarını Ekleme (AddRoundKey)
   - Anahtar Üretim bloğunun ürettiği anahtar ile veri toplanır.
   - Her bit için (XOR) işlemine denk gelir.

Anahtarların Üretilmesi (GenerateithKey)

- Üretim bloğu, anahtar uzunluğunu bit dizilerinin uzunluğuna göre matrislere çevirir.
- Tur sayısı N; matris boyutu: 4xK.
  Yapılacak işlemlerle genişlemiş matrisin boyutu: 4x(K*(N+1))

AES şifrelemede CBC ve OFB modları da eklenerek gerçeklenmiştir.

CBC modu (Cipher Block Chaning)

Her blok, kendisinden sonraki blok ile XOR işlemine tabi tutulur ve öyle şifreleme işlemine geçilir. Önceki blokla işleme tabi tutulduğu için döngüler birbirine bağlıdır ve çözümü daha zordur. İlk blok IV adı verilen ilklendirme vektörü ile işleme girer.

$$C_i = E_K(P_i \oplus C_{i-1}), C_0 = IV \qquad P_i = D_K(C_i) \oplus C_{i\ 1}, C_0 = IV.$$

OFB modu (Output Feedback Mod)

$$C_j = P_j \oplus O_j,$$
$$P_j = C_j \oplus O_j,$$
$$O_j = E_K(I_j),$$
$$I_j = O_{j\ 1},$$
$$I_0 = \mathrm{IV}.$$

Metni verilere bölerek metin üzerinde değil, vektör ve anahtar üzerinde çalışır. Şifrelemeden sonra metin ile XOR işlemine tabi tutulur.

Deşifreleme ve test işlemleri de yapılmıştır.

Test:

```
cse312@ubuntu:~/Desktop/crypto/141044049$ make
python test.py aes.py
m=2,
ol=37 (37),
cipher=[107, 184, 248, 88, 219, 147, 211, 5, 17, 134, 217, 249, 254, 30, 145, 24
0, 32, 145, 189, 70, 241, 221, 61, 149, 110, 58, 116, 32, 0, 67, 121, 133, 91, 8
1, 234, 22, 101, 143, 145, 77, 19, 59, 182, 44, 179, 170, 203, 155]
Ebru Kardas Gebze Teknik Universitesi



('Mode:', 'CBC')
('cleartext:','Ebru Kardas Gebze Teknik Universitesi')
Cipher: [96, 2, 31, 9, 10, 1, 110, 129, 195, 218, 45, 2, 241, 224, 119, 121, 219
, 50, 102, 57, 162, 39, 49, 172, 159, 91, 222, 75, 152, 27, 96, 179, 12, 36, 42,
 64, 220, 238, 58, 106, 165, 133, 190, 176, 148, 2, 204, 4, 8, 96, 102, 177, 34,
 160, 91, 163, 71, 246, 163, 168, 99, 135, 62, 174]
Plain: Ebru Kardas Gebze Teknik Universitesi



('Mode:', 'OFB')
('cleartext:', 'Ebru Kardas Gebze Teknik Universitesi')
Cipher: [69, 139, 255, 216, 250, 234, 61, 12, 235, 27, 129, 239, 91, 255, 70, 10
2, 157, 222, 154, 118, 81, 98, 197, 99, 228, 56, 150, 99, 10, 59, 166, 3, 6, 75,
 234, 205, 91, 111, 242, 58, 36, 20, 100, 30, 50, 236, 245, 242, 114, 110, 125,
105, 229]
Plain: Ebru Kardas Gebze Teknik Universitesi
cse312@ubuntu:~/Desktop/crypto/141044049$
```