**22100011028**

**Reşide ALTUN**

**KRİPTOLOJİ DERSİ - PROJE SUNUMU**

**KONU: AES + Hill Cipher**

**AES (Advanced Encryption Standard)**

**AES, yani Gelişmiş Şifreleme Standardı, günümüzde en yaygın kullanılan simetrik anahtarlı blok şifreleme algoritmasıdır. Simetrik şifreleme demek, hem şifreleme hem de şifre çözme işlemlerinin aynı anahtarla yapılması anlamına gelir.**

**Blok Tabanlı Çalışma Yapısı:**

**AES, veriyi 128-bitlik (16 byte) bloklar halinde işler. Yani, metin ne kadar uzun olursa olsun, şifreleme işlemi 16 baytlık parçalar halinde yapılır. Her bir blok, belirli sayıda dönüşümden (round) geçirilerek şifrelenir.**

**AES Türleri ve Anahtar Uzunlukları**

**AES algoritmasının üç farklı versiyonu vardır ve bu fark, kullanılan anahtar uzunluğuna göre belirlenir:**

| **AES Versiyonu** | **Anahtar Uzunluğu** | **Tur (Round) Sayısı** |
| --- | --- | --- |
| **AES-128** | **128 bit (16 byte)** | **10 tur** |
| **AES-192** | **192 bit (24 byte)** | **12 tur** |
| **AES-256** | **256 bit (32 byte)** | **14 tur** |

**Her bir tur, blok üzerinde SubBytes, ShiftRows, MixColumns ve AddRoundKey gibi çeşitli matematiksel işlemlerle veriyi karıştırır ve güvenli hale getirir.**

**Neden AES?**

**AES, 2001 yılında eski algoritma olan DES'in (Data Encryption Standard) güvenliğinin zayıflamasıyla birlikte resmi şifreleme standardı olarak kabul edilmiştir. Gerek hız, gerek güvenlik açısından AES, günümüzde hem devlet kurumlarında hem de özel sektör uygulamalarında yaygın olarak kullanılmaktadır.**

**Özellikler:**

* **Simetrik anahtar kullanır.**
* **Sabit blok boyutu: 128 bit.**
* **Güçlü ve hızlıdır.**
* **Hem yazılım hem donanımda verimli çalışır.**
* **Kırılması günümüz teknolojisiyle çok zordur.**

**Hill Cipher Nedir?**

**Hill Cipher, 1929 yılında Lester S. Hill tarafından geliştirilen bir matematiksel şifreleme algoritmasıdır. Polialfabetik bir yerine koyma (substitution) yöntemidir ve şifreleme işlemi matris çarpımına dayanır.**

**Temel Yapısı**

**Hill Cipher'da:**

1. **Harfler sayılara çevrilir (A=0, B=1, ..., Z=25).**
2. **Metin 2'li veya 3'lü bloklara ayrılır (anahtar matris boyutuna göre).**
3. **Her blok, bir anahtar matrisiyle çarpılır.**
4. **Elde edilen sonuçlar mod 26 (İngiliz alfabesi için) alınarak tekrar harfe çevrilir.**
5. **Böylece şifreli metin elde edilir.**

**Şifreleme Formülü**

**C=K⋅P mod  26**

* **C: Şifreli blok (ciphertext)**
* **K: Anahtar matrisi**
* **P: Düz metin bloğu (plaintext)**
* **mod 26: Sonuçları 0-25 arası sınırlamak için (İngiliz alfabesi 26 harf)**

**Şifre Çözme Formülü**

**P= -1K ⋅ C mod  26**

* **-1K: Anahtar matrisin mod 26 tersidir.**
* **Bu ters matris varsa (yani determinantı mod 26'ya göre terslenebiliyorsa), çözme mümkündür.**

**Anahtar Matris**

* **Anahtar, genellikle 2x2 veya 3x3 bir mod 26 tamsayı matrisidir.**
* **Matrisin determinantı, mod 26 altında sıfır olmamalı ve terslenebilir olmalıdır. (Yani gcd(det, 26) = 1 olmalı.)**

**Özellikler**

* **Şifreleme matematiksel ve hızlıdır.**
* **Aynı anda birden çok harfi şifreleyebilir (blok şifreleme mantığı).**
* **Anahtar değiştikçe şifre de tamamen değişir.**
* **Anahtar kötü seçilirse şifre çözülemez olabilir.**
* **Modern güvenlik standartlarına göre kırılması kolaydır, ama eğitimsel amaçlar için çok faydalıdır.**

**AES+ HİLL CİPHER ÖRNEK ÇÖZÜMÜ**

1. Orijinal Metin: HELLO WORLD
2. AES ile Şifreleme (ECB Modu, 128-bit rastgele anahtar):

AES algoritması bu metni 16 byte’a (128 bit) padding’le tamamla ve şifrele.

* AES Şifrelenmiş (bytes olarak):

[151, 39, 22, 36, 255, 106, 87, 148, 35, 6, 65, 11, 110, 223, 188, 6]

* AES Şifrelenmiş (ASCII karakter olarak):

"\x97'\x16$ÿjW\x94#\x06A\x0bnß¼\x06"

Not: Bu karakterlerin çoğu ekranda görünmeyen veya özel anlam taşıyan byte’lar olabilir.

3. Hill Cipher ile Şifreleme:

AES şifrelemesinden gelen 16 karakter, 2'li gruplar halinde 8 vektöre bölünür. Bu vektörler, [[3, 3], [2, 5]] anahtar matrisiyle çarpılarak mod 256 alınır. Böylece Hill Cipher uygulanmış olur.

Hill Cipher ile Şifrelenmiş Metin:

:ñ®àFbÁ{dä¹ã;-RÄ

Bu metin artık çift katmanlı şifreli hale gelmiştir.

4. Hill Cipher ile Şifreyi Çöz:

Hill Cipher ters matris kullanılarak çözülür. Bu işlem sonucunda tekrar AES çıktısına ulaşılır.

Hill çözülmüş hali (AES formatı):

"\x97'\x16$xJW\x94#\x06A\x0bNSS¼\x06X"

Bu değer, şifreleme sırasında elde edilen AES çıktısına çok yakındır (karakter farkı padding veya byte çevrimi kaynaklı olabilir).

5. AES ile Şifreyi Çöz:

AES şifresi çözüldüğünde orijinal metin ortaya çıkar.

Sonuç:HELLO WORLD