İSTANBUL BEYKENT ÜNİVERSİTESİ
BİLGİSAYAR MÜHENDİSLİĞİ YÜKSEK LİSANSI
2023-2024

AES ŞİFRELEME ve GÜVENLİĞİ

Gökhan YILMAZ
2220003096

İÇİNDEKİLER

Kriptoloji Nedir?

- Kriptoloji, haberleşen iki veya daha fazla tarafın bilgi alışverişini emniyetli olarak yapmasını sağlayan, temeli matematiksel zor problemlere dayanan teknik ve uygulamaların bütünüdür.
- Günümüzde kriptoloji, matematik, elektronik, optik, bilgisayar bilimleri gibi birçok alanda kullanılan bir bilim dalı olarak kabul edilmektedir.

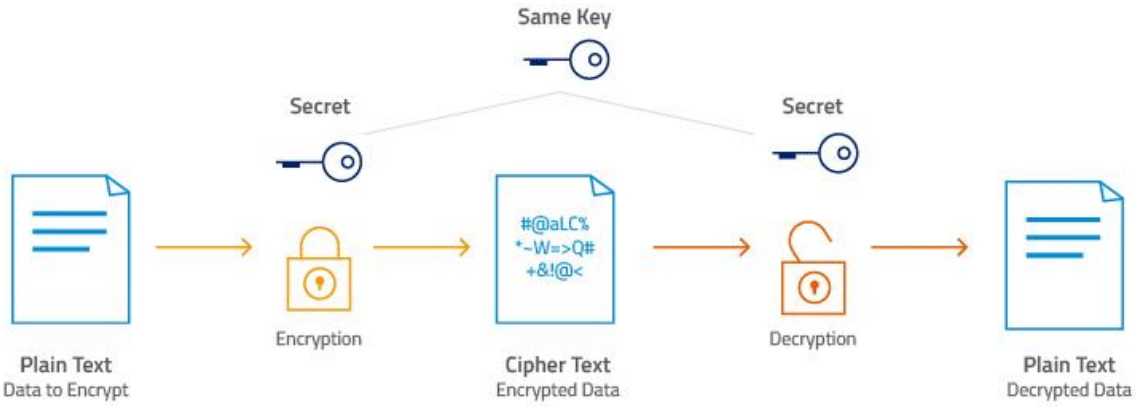
Kriptolojinin iki temel alt dalı vardır:

- Kriptografi
- Kriptoanaliz
- Kriptografi, belgelerin şifrelenmesi ve şifresinin çözülmesi için kullanılan yöntemlere verilen addır.
- Kriptoanaliz, kriptografik sistemlerin kurduğu mekanizmaları inceler ve çözmeye çalışır. Kriptoanalizin kriptoloji önemi çok büyüktür çünkü ortaya konan bir şifreleme sistemini inceleyerek, zayıf ve kuvvetli yönlerini ortaya koymak için kriptoanaliz kullanılır.

AES Şifreleme Nedir?

AES (Advanced Encryption Standard-Gelişmiş Şifreleme Standardı)

- Digital ortamdaki verilerin şifrelenmesi amacıyla sunulmuş olan bir sistemdir.
- AES uluslararası standartlara uygun kabul görmüş bir şifreleme metodudur. Sunduğu güvenlik ve koruma miktarı açısından benzersizdir.
- AES ile tanımlanan şifreleme algoritması, hem şifreleme hem de şifreli metni çözmede kullanılan anahtarların birbiriyle ilişkili olduğu, simetrik-anahtarlı bir algoritmadır. AES için şifreleme ve şifre çözme anahtarları aynıdır.



AES, teknoloji dünyasında "blok şifresi" olarakta geçer.

Buna "blok" denir çünkü bu tür bir şifre şifrelenecek bilgileri böler (düz metin olarak bilinir) blok adı verilen bölümlere ayırır.

Daha spesifik olmak gerekirse, AES bir 128 bit blok boyutu.

Bu, verilerin bir bölüme ayrıldığı anlamına gelir. dörde dört dizi 16 bayt içerir. Her bayt sekiz bit içerir.

Bu nedenle, 16 bit ile çarpılan 8 bayt, bir sonuç verir. her blokta toplam 128 bit.

Bu bölünmeden bağımsız olarak, şifrelenmiş verilerin boyutu aynı kalır. Başka bir deyişle, 128 bit düz metin, 128 bit şifreli metin verir.

AES' in Tarihçesi

- ABD Ulusal Standart ve Teknoloji Enstitüsü (NIST) tarafından 26 Kasım 2001 tarihinde US FIPS PUB 197 kodlu dokümanla duyurulmuştur.
- 5 yıllık bir sürede standartlastırılmıştır. Bu 5 yıllık zaman süresinde AES'in yerine geçebilecek 15 farklı tasarım öne sürülmüştür. Ancak bu tasarımlar güvenlik ve performans açısından değerlendirildikten sonra başarısız olmuşlardır.
- Bu sebeple AES en iyi şifreleme standardı olarak seçilmiştir.
- NSA tarafından çok gizli bilgilerin şifrelenmesinde kullanılması onaylanmış olan ilk kamuya açık şifreleme algoritmasıdır.

AES ile standartlaştırılan algoritma, esas olarak **Vincent Rijmen** ve **Joan Daemen** tarafından geliştirilen **Rijndael** algoritmasında bazı değişiklikler yapılarak oluşturulmuştur. Rijndael, geliştiricilerin isimleri kullanılarak elde edilen bir isimdir: **RIJmen aNd DAEmen**.

Vincent Rijmen ve **Joan Daemen**

AES Algoritmasının Genel Yapısı

- AES algoritması; hem şifreleme hem de şifre çözmede kullanılacak anahtarların simetrik ilişkili olduğu bir algoritmadır. Şifreleme ve çözme anahtarları aynıdır.
- AES performans olarak; yüksek hız ve ram de düşük yer kaplar.
- AES Değiştirme-Karıştırma(Subsititution-Permutation) yapısında oluşturulan bir algoritmadır. AES'in hem yazılımsan hem donanımsal olarak performansı oldukça yüksektir.128-bit girdi bloğu,128,192 ve 256 bit anahtar uzunluğuna sahiptir.
- AES'in temel alındığı Rijndael ise 128-256 bit arasında 32'nin katı olan girdi blok uzunluklarını ve 128 bitten uzun anahtar uzunluklarını desteklemektedir. Dolayısıyla, standartlaşma sürecinde anahtar ve girdi blok uzunluklarında kısıtlamaya gidilmiştir.
- AES, durum (state) denilen 4x4 sütun-öncelikli bayt matrisi üzerinde çalışır.
- Algoritma belirli sayıda tekrar eden girdi açık metni, çıktı şifreli metne dönüştüren özdeş dönüşüm çevrimlerinden (raund) oluşmaktadır. Her çevrim, son çevrim hariç, dört adımdan oluşmaktadır. Şifreli metni çözmek için bu çevrimler ters sıra ile uygulanır. Çevrimlerin tekrar sayıları 128-bit, 192-bit ve 256-bit anahtar uzunlukları için sırası ile 10, 12 ve 14'tür.
- Anahtar uzunluğu bit sayıları arasındaki farklılık AES tur döngülerinin sayısını değiştirmektedir.

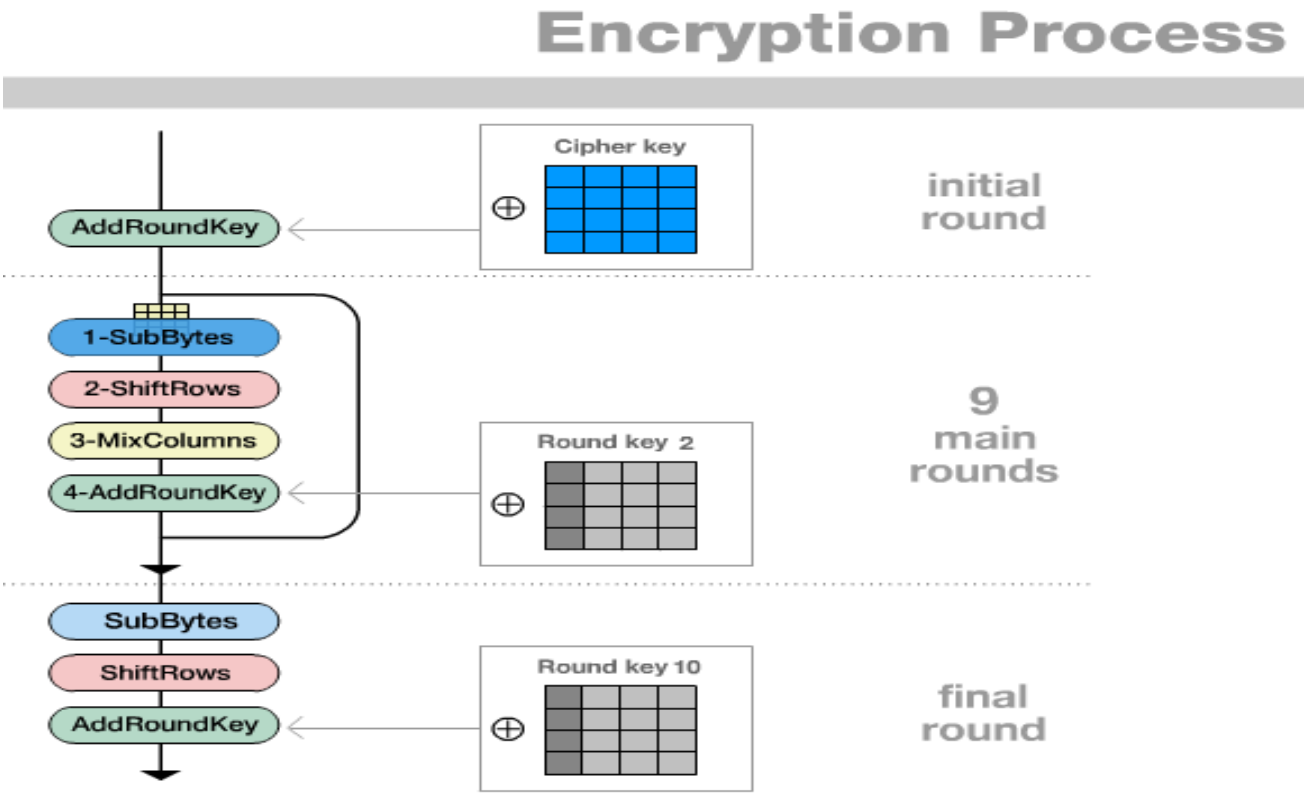
	Kelime Uzunluğu	Tur Sayısı
Aes-128	4	10
Aes-192	6	12
Aes-256	8	14

Neden AES-256

- Güvenlik
- Hızlı çalışması
- Daha Az Hafıza ile Çalışması
- Donanım ve Yazılıma Uygun Olabilmesi
- Esneklik

AES Nasıl Çalışır?

- AES, üç ana adımdan oluşur: Anahtar genişletme, Şifreleme ve Şifre Çözme
- AES'in anahtar genişletme adımı, kullanıcının girdiği anahtardan bir dizi alt anahtar oluşturur. Bu alt anahtarlar, şifreleme ve şifre çözme işlemleri sırasında kullanılacaktır.
- Şifreleme adımı, veriyi önceden belirlenmiş boyutlarda bloklar halinde ayırır ve her bloğu aynı anahtar kullanarak şifreler. Bu işlem, blokların karıştırılması, değiştirilmesi ve yer değiştirmeleri gibi bir dizi matematiksel işlemi içerir. Şifreleme işlemi tamamlandıktan sonra, şifrelenmiş veri güvenli bir şekilde aktarılabilir.
- Şifre çözme adımı, şifrelenmiş veriyi alır ve aynı anahtar kullanarak şifreyi çözer. Şifre çözme adımı, şifreleme adımının ters işlemi olarak çalışır ve şifrelenmiş verinin orijinal haline dönüştürülmesini sağlar.



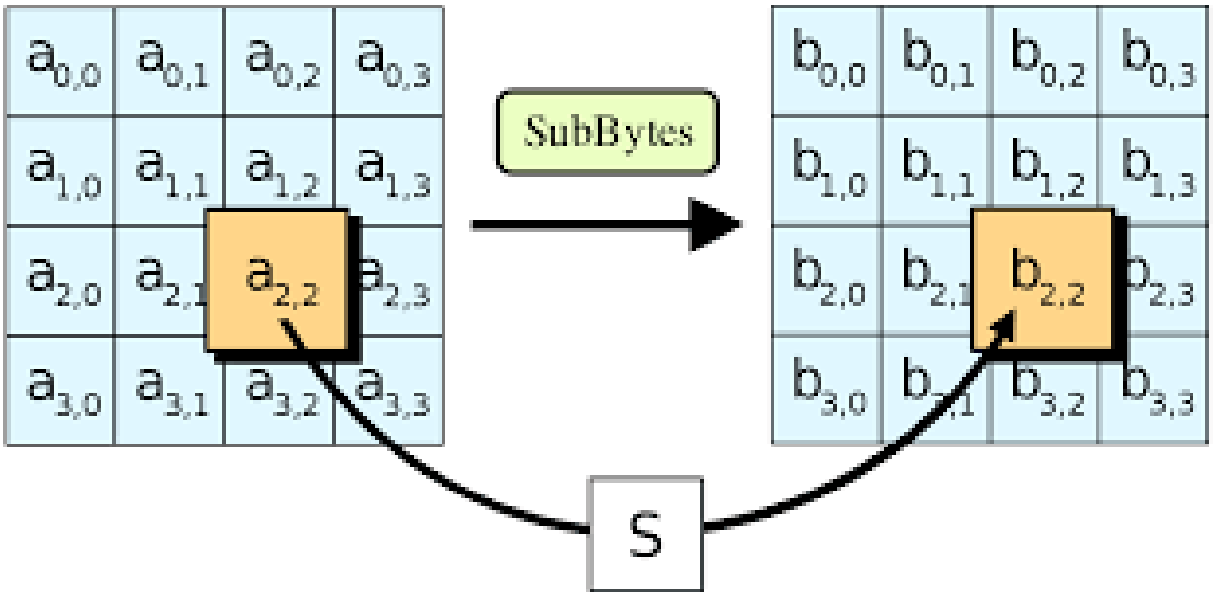
-AES ALGORİTMASI-

Her çevrim, son çevrim hariç, dört adımdan oluşmaktadır;

- Bayt Değiştir (SubBytes) Adımı
- Satır Kaydır (ShiftRows) Adımı
- Sütun Karıştır (MixColumn) Adımı
- Anahtar Ekle (AddRoundKey) Adımı

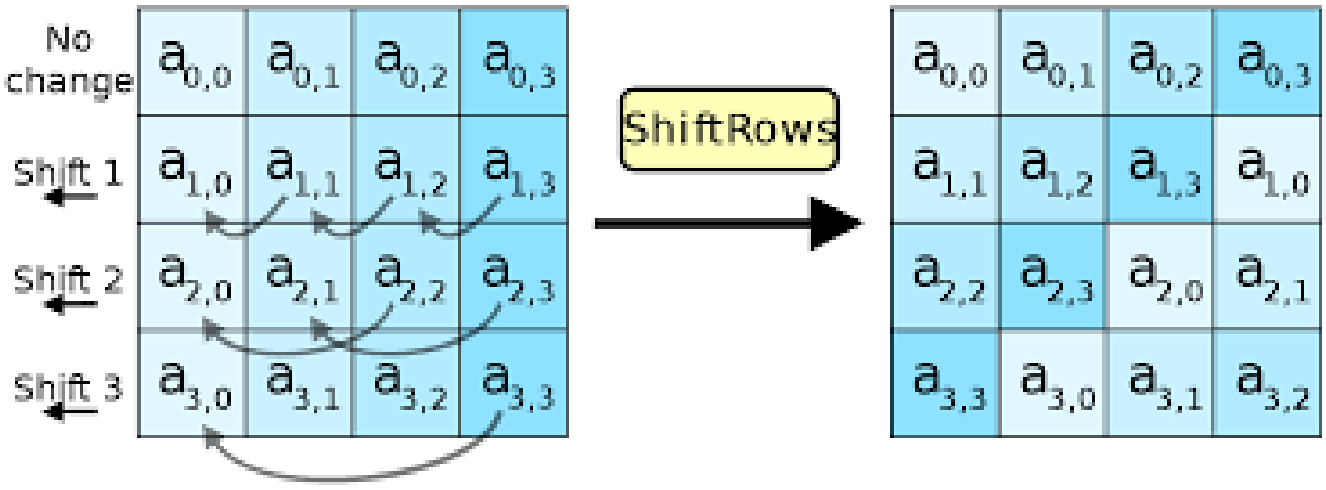
Bayt Değiştir (SubBytes) Adımı

Matristeki her baytın değeri, 8 bitlik bir değişim kutusu (substitution box) kullanılarak güncellenir. Bu adım algoritmanın doğrusallığını bozar ve doğrusal-olmayan (non-linear) bir dönüşüm hâline gelmesini sağlar. Kullanılan değişim kutusu yüksek doğrusal-olmayanlık (nonlinearity) özelliğine sahip olduğu bilinen, sonlu cisim GF (28) üzerinde ters alma işleminden elde edilmiştir. Cebirsel özellikler kullanan saldırılara karşı dayanıklı olası için sonlu cisim üzerinde ters alma işlemine tersi olan doğrusal bir dönüşüm daha eklenmiştir. Ayrıca değişim kutusu herhangi bir sabit nokta veya ters sabit nokta olmayacak şekilde seçilmiştir.



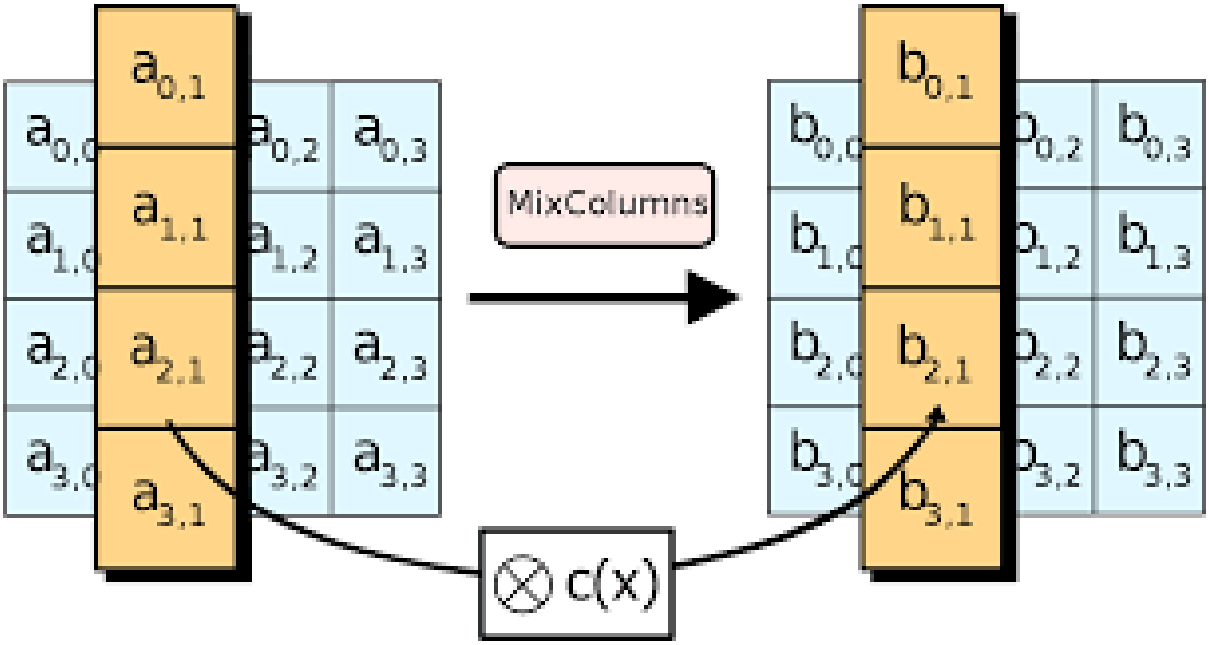
Satır Kaydır (ShiftRows) Adımı

Matrisin satırları üzerinde çalışan bu işlem her satırdaki bayt değerlerini belirli sayıda kaydırır. AES'de ilk satır sabit kalırken 2., 3. ve 4. satırlar sırası ile 1, 2 ve 3 bayt sola kaydırılır. Rijndael algoritmasında ise 256-bit için bu değerler, ilk satır sabit kalacak şekilde 1, 3 ve 4 bayttır.



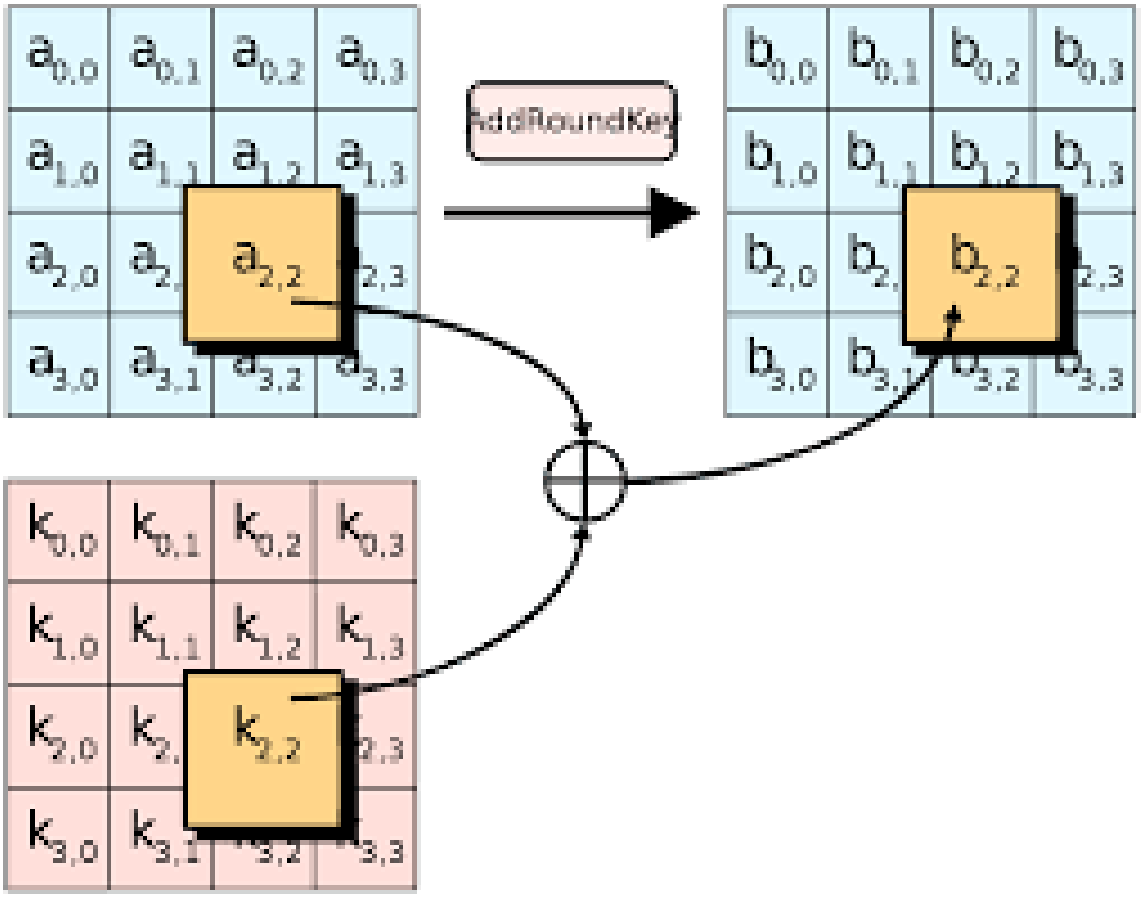
Sütun Karıştır (MixColumn) Adımı

Bu adımda her sütundaki dört bayt değeri tersi olan doğrusal bir dönüşüm kullanılarak birbirleriyle karıştırılır. Sütun Karıştır fonksiyonu 4 bayt girdi alıp 4 bayt çıktı verir ve girdideki her baytın çıktıdaki her bayt değerini etkilemesini sağlar. Sütun Karıştır işlemi, her sütunun sabit bir matrisle çarpılması işleminden oluşur.



Anahtar Ekle () Adımı

Bu adımda çevrim anahtarı durum matrisi ile kaynaştırılır. Çevrim anahtarı baytlara bölündükten sonra sıra ile matrisin elemanları ile XOR'lanır.



AES Algoritmasının Güvenliği

- 256-bit'lik bir anahtarın kullanıldığı şifrelemenin çözülebilmesi için oldukça zor olduğunu düşünürsek şu an için bu şifrenin kırılması için gereken süre evrenin yaşından fazla olacaktır.
- AES algoritmasının 128,192 ve 256 bitlik şifrelemeleri GİZLİ statüsünde olan veriler için uygun olarak belirtilmiştir. Fakat ÇOK GİZLİ statüsünde olan veriler için ise 192 veya 256 bitli şifreleme kullanılması gerektiği belirtilmiştir. Önemli verilerin korunması gereken ürünlerdeki AES uygulamalarının kullanıma sunulmadan önce NSA tarafından incelenip sertifikalandırılmalıdır**.**

AES' Yapılan Saldırılar

XSL Saldırısı

2002 yılında AES'in sade ve basit cebirsel yapısını değerlendiren Nicolas Courtois ve Josef Pieprzyk "XSL Attack" isimli bir teorik saldırı duyurmuşlardır. Ancak daha sonra, duyurulan hâliyle atağın çalışmadığını gösteren bilimsel yayınlar yapılmıştır.

İlişkili Anahtar Saldırısı

- 1 Temmuz 2009 ilan edilmiştir.
- Bruce Schneier blogunda 192-bit ve 256-bit AES versiyonlarına Alex Biryukov ve Dmitry Khovratovich tarafından 2^{119} işlem karmaşıklığı ile uygulanabildiğini söylenmiştir
- Aralık 2009'da bu saldırının işlem karmaşıklığı $2^{99.5}$e düşürülmüştür. Ardından Alex Biryukov, Orr Dunkelman, Nathan Keller, Dmitry Khovratovich ve Adi Shamir 9 çevrim AES-256'ya sadece iki ilişkili-anahtar kullanarak 2^{39} zamanda anahtarın tamamının elde edildiği saldırıyı yayımlamışlardır
- Bu saldırı 2^{45} zaman karmaşıklığı ile 10 çevrime, 2^{77} zaman karmaşıklığı ile 11 çevrime genişletilmiştir ancak tam çevrim AES bu ataktan etkilenmemiştir.

Biclique Saldırısı

- İlk şifre anahtarı ele geçirme saldırısıdır.
- 128-bit anahtarı $2^{126.1}$, 192-bit anahtarı $2^{189.7}$ ve 256-bit anahtarı $2^{254.4}$ işlem karmaşıklığı ile elde etmektedir.
- Teorik olarak yapılmıştır
- Aes bundan etkilenmemiştir

Donanım Saldırıları

2005 yılında D.J. Bernstein OpenSSL'in AES uygulamasını kullanan bir sunucuya ön bellek-zamanlama (cache-timing) saldırısı yapmıştır. 200 milyon civarında seçilmiş açık metin kullanılarak yapılan saldırıda, sunucu şifreli metinle birlikte şifrele işleminin kaç işlemci saati sürdüğünü de alıcıya göndermekteydi. Bernstein, bu saldırının başarılı olması için, şifreleme süresinin sunucudan gelen kadar kesin olmasına gerek olmadığını göstermiştir.

AES'in Kullanım Alanları

- Bugün, dahil olmak üzere çok sayıda programlama dili için AES kitaplıkları oluşturulmuştur. C, C++, Java, Javascript ve Python.
- Whatsapp , Facebook Messenger vb. gibi mesajlaşma uygulamaları AES şifreleme standardını kullanmaktadır.
- Dosya sıkıştırma programları: 7 Zip, WinZip ve RAR dahil ve disk şifreleme sistemleri BitLocker ve FileVault gibi; ve NTFS gibi dosya sistemleri.
- Bilgisayar Donanımlarında; Tüm intel ve Amd işlemciler
- Video oyunlarında kullanılıyor hackerlardan korunmak için
- Birçok finans kuruluşunun finans uygulamalarında

AES kullanmaktadırlar.

Kaynakçalar

https://tr.wikipedia.org/wiki/AES

https://www.academia.edu/

https://chat.openai.com/

https://consensus.app/search/

https://www.atpinc.com/blog/what-is-aes-256-encryption

https://www.samiam.org/key-schedule.html

https://www.youtube.com/watch?v=vFXgbEL7DhI

https://digitalguardian.com/blog/social-engineering-attacks-common-techniques-how-prevent-attack

https://www.consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams