GELİŞMİŞ ŞİFRELEME STANDARDI - AES

Şifreleme algoritmalarına yapılan saldırılarda kullanılan yöntemin dayanıklı olması o algoritmanı gücünü gösterir. Aes'in ortaya çıkışının temelinde Des şifreleme algoritmasının saldırılara karşı dayanıksız olması yatar. 1997'de RSA Security firması yapmış olduğu bir konferansta İngilizce bir cümle, Des ile şifrelenerek internete konuldu. Ardından kırabilecek olan ilk kişiye 10,000 dolar şeklinde ödül vereceklerini söylediler. 56 bit uzunluğundaki bu anahtar güçlü bilgisayarların bir araya gelmesi ile kırılmış oldu. Kriptografi uzmanları olan Joan Daemen ve Vincent Rijmen tarafından geliştirilmiş 128, 192, 256-bitlik anahtar uzunluğu seçeneklerine sahip olan Rijndael algoritması, Gelişmiş Şifreleme Standardı (AES) ismiyle elektronik ortamda veri güvenliğini sağlanması amacıyla veri şifreleme standardı olarak ortaya konulmuştur.

AES günümüzde hala güvenirliliğini korumakta ve bilişim dünyasında güvenlik için kullanılmaktadır. Günümüz teknolojisinde ürün boyutunun küçük olması aynı zamanda hızlı olması tercih edilen özelliklerdendir. Bundan dolayı AES'in en az sayıda bellek kullanması ve yeterli hızda olması gerekmektedir. Kriptografik işlemcide kullanılan algoritmalar, yazılımsal ve donanımsal olarak gerçeklenebiliyorlar. Yazılımla yapılmış olan gerçeklemeler daha az maliyete ve esnekliğe sahipken donanımsal gerçeklemeler hızlı çalışır ve daha güvenilirdir.

Rijndael Algoritması

Rijndael algoritması, sahip olduğu anahtarlara göre farklı sayıda döngüsel işlemler yapar. Her döngü sonunda anahtar yenilenir veriye uygulanır. Veri öncelikle diziler şeklinde ifade edilir. Diziler numaralandırılırken sıfırıncı indeksle başlanır ve dizi uzunluğunun bir eksiği ile sonlandırılır. AES 128-bitlik düz metni şifrelerken de yine 128-bitlik şifrelenmiş metni çözerken de aynı anahtarı kullanır. 128 bit uzunluğunda olan veri, (4x4) 'lük matrislere bölünerek algoritmaya dahil olur. Bu matrisin her bir elemanı 8 bit boyutunda olup her bir satır veya sütun 32 bite sahiptir. Bu matrise "durum" denilir ve her bir satırı kelime olarak adlanırılır. AES şifrelerken kullanacağı algoritmada anahtarın uzunluğuna göre döngü sayısının atamasını yapar. Bu döngüsel işlemin artmasıyla veri daha çok güvenilir hale gelir. Fakat aynı zamanda yapılacak olan döngüsel işlemlerin de artmasıyla hem işlem sayısı artar hem de bellek alanı artar.

Şifrelemeyi oluşturacak anahtar da aynı zamanda durum dediğimiz matris haline çevrilir. Aes şifreleme algoritması, bu durum matrislerinin üzerinde işlemlerini gerçekleştireceğinden veri en elverişli şekilde çevrilmelidir. Şifreleme başlangıcı düz metne ait durum matrisi ile anahtara ait durum matrisinin toplanmasıyla yapılır.

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

BAYTLAR

AES algoritmasının en küçük parçası, durum matrisinin elemanı 8-bitlik diziden oluşan bayttır. Şifrelenecek metin, şifreleme anahtarı ve şifrelenmiş metin, baytlar ile bir araya gelerek bayt dizilerine dönüşüyor. Bu bayt dizilerinin uzunluğu anahtarının uzunluğuna göre doğrusal olarak değişiyor. Böylece matris boyutu da değişmiş oluyor. Matris eleman sayısı n ile tanımlanırsa, n sayısı anahtarın uzunluğuna göre değişiklik gösterir.

Anahtar uzunluğu = 128 bit, 0< n< 16;
Anahtar uzunluğu = 192 bit, 0< n<24;
Anahtar uzunluğu = 256 bit, 0< n<32;

AES algoritmasında aşağıdaki polinom temsili ile sonlu alan elemanı: {b7, b6, b5, b4, b3, b2, b1, b0} şeklindeki bayt değerleri ile tanımlanır.

$$b_7x^7 + b_6x^6 + b_5x^5 + b_4x^4 + b_3x^3 + b_2x^2 + b_1x + b_0 = \sum_{i=0}^{7} b_i x^i$$

Örneğin : {10100011} baytı sonlu alan elemanı $x^7 + x^5 + x + 1$ 'i
{01100011} baytı sonlu alan elemanı $x^6 + x^5 + x + 1$ 'i belirtir.

Ayrıca bayt değerlerini onaltılık tabanda göstermek mümkündür. İlk dört bit ve son dört bit birer hexadecimal karakterle gösterilir.Karakterlerin ikilik düzendeki karşılıkları aşağıdaki gibi olur.

$(0000)_2=(0)_{16}$
$(0001)_2=(1)_{16}$
$(0010)_2=(2)_{16}$
$(0011)_2=(3)_{16}$
$(0100)_2=(4)_{16}$
$(0101)_2=(5)_{16}$
$(0110)_2=(6)_{16}$

$(0111)_2 = (7)_{16}$

$(1000)_2 = (8)_{16}$

$(1001)_2 = (9)_{16}$

$(1010)_2 = (A)_{16}$

$(1011)_2 = (B)_{16}$

$(1100)_2 = (C)_{16}$

$(1101)_2 = (D)_{16}$

$(1110)_2 = (E)_{16}$

$(1111)_2 = (F)_{16}$

“19 A0 9A E9 3D F4 C6 F8 E3 E2 8D 48 B3 2B 2A 08” bu şekilde yani onaltılık tabanda ifade edilmiş 16 tane 8’er bitlik diziyi şifrelemek için, verinin durum matrisi haline getirilmesi gerekir.
İlk dört eleman, matrisin ilk sütunundan başlanarak yerleştirilir. Oluşan matris aşağıdaki gibidir.

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