GELİŞMİŞ ŞİFRELEME STANDARDI - AES

Şifreleme algoritmalarına yapılan saldırılarda kullanılan yöntemin dayanıklı olması o algoritmanın 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**

DÖNGÜ YAPISI

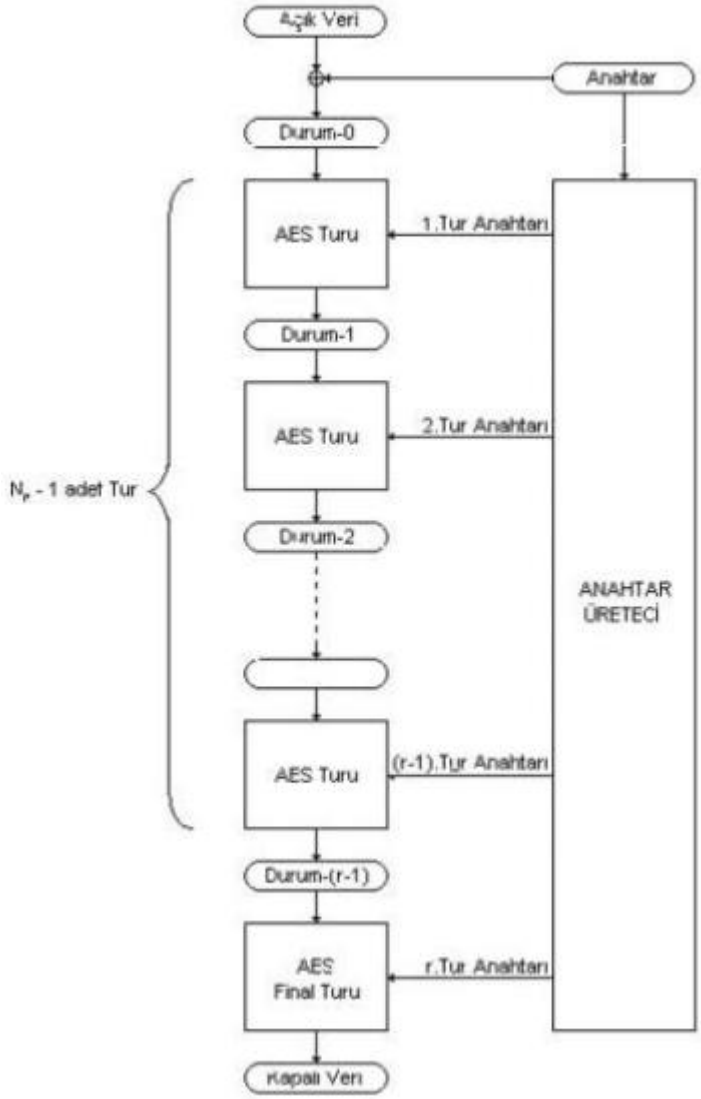
Durum matrisinin oluşumuyla algoritma yürürlüğe girer. Aes algoritmasının döngü kullanarak işlem yapması algoritmayı güçlü yapan bir özelliktir. Aes algoritması sırasıyla bayt değiştirme, satır kaydırma, sütun karıştırma ve tur anahtarı ile toplama işlemlerini gerçeklemesiyle şifrelenmiş veriyi elde eder ve tekrar bayt değiştirme adımına döner. Döngü sayısı anahtar uzunluğuna göre değişir. Sadece son döngüde sütun karıştırma işlemi yapılmaz, tur anahtarı ile toplama işlemi yapılır ve şifrelenmiş blok elde edilir Şifrelenmiş veriyi çözerken de bu alt işlemlerin tersi uygulanır.
Döngüler durum matrislerinde 4 dönüşüm uygular.

- SubBytes
- ShiftRows,
- MixColumns
- AddRoundKey.

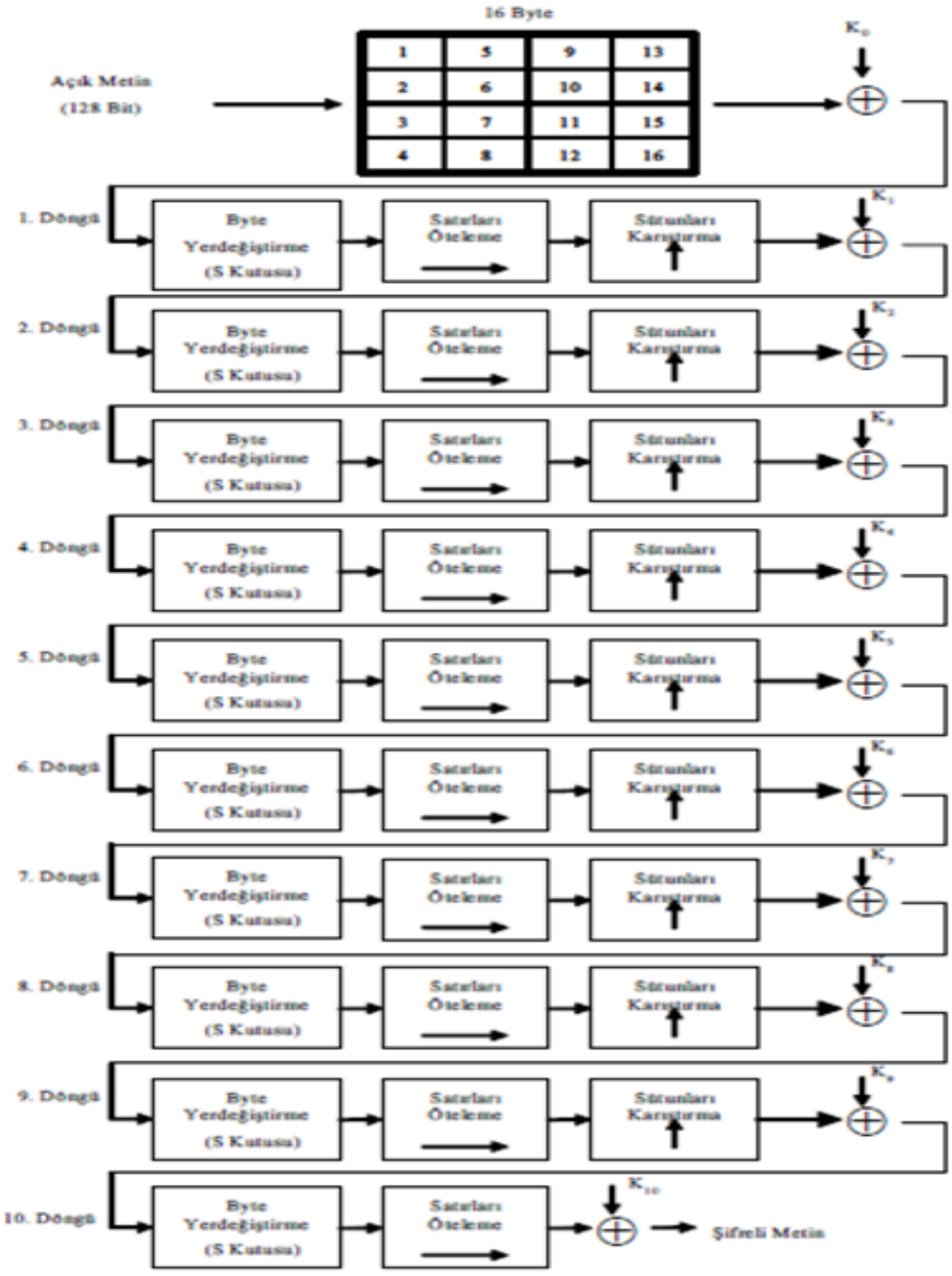
Her döngüde işleme farklı anahtar materyali sokulur. Bu farklı anahtarlar, başlangıçta belirlenen anahtardan anahtar oluşumu işlemleri sırasında üretilirler.

Şifre Çözme kısmında kullanılan ters dönüşümler:

- InvSubByte
- InvShiftRows
- InvMixColumns
- AddRounKey (tersi kendisidir- XOR işlemi)

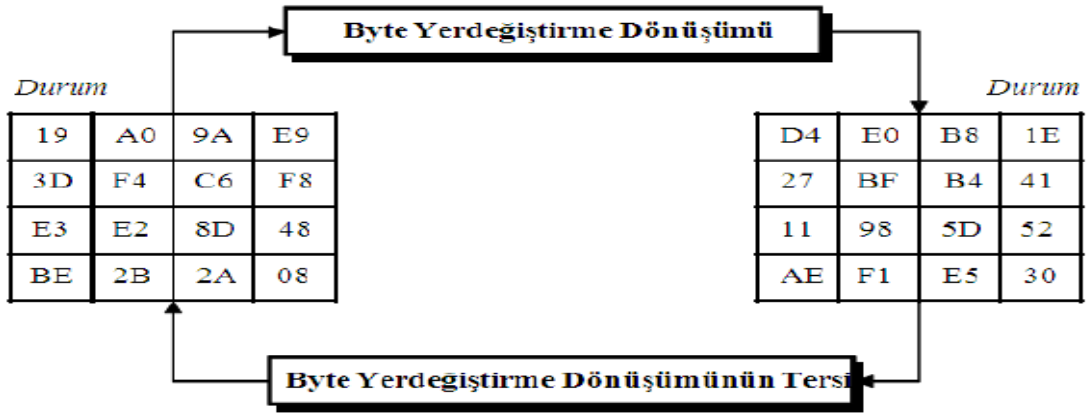


AES BLOK ŞEMASI


16 Byte
Açık Metin
(128 Bit)
1 5 9 13
2 6 10 14
3 7 11 15
4 8 12 16
K0
1. Döngü
2. Döngü
3. Döngü
4. Döngü
5. Döngü
6. Döngü
7. Döngü
8. Döngü
9. Döngü
10. Döngü
Byte Yerdeğiştirme (S Kutusu)
Satırları Öteleme
Sütunları Karıştırma
K1
K2
K3
K4
K5
K6
K7
K8
K9
K10
Şifreli Metin

BAYT DEĞİŞTİRME

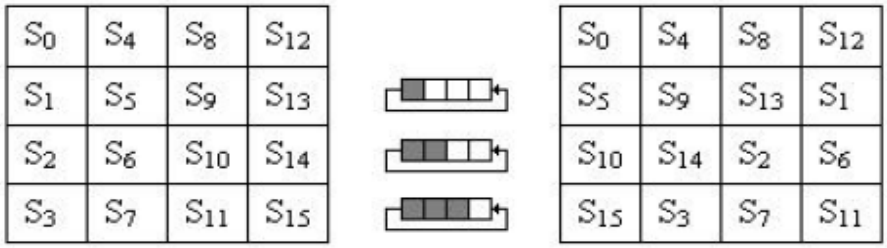
Döngünün ilk gerçekleştirilen işlemi ve algoritmanın tek doğrusal olmayan işlemidir. Bit dizilerinden elde edilen durum matrisi bu aşamada eleman değişikliğine uğrar. Değişiklik değerleri önceden hesaplanmış S-Kutusuna göre yapılır. S-Kutusu, durum matrisinin elemanları onaltılık tabana göre oluştuğu için 16x16 boyutunda bir matristir denebilir. 16 satırdan ve 16 sütunda oluşur. Satır ve sütun göstergeleri onaltılık tabanda "0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F" elemanları ile yapılır. Örneğin aşağıda solda yer alan durum matrisinin ilk elemanı 19'u S-Kutusuna bakarak değiştiririz. Bu bayt değiştirme işleminde, S-Kutusunun satırları gösteren 1. indeksine ve sütunları gösteren 9. indeksine bakılır oradaki değer 19'un yer aldığı yere yazılır. Bu değer aşağıdaki S-Kutusunda D4'tür. Bu işlem matrisin tüm elemanlarına uygulanır ve yeni bir durum matrisi elde edilir.



	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
6	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
8	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
A	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
B	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
C	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
D	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
E	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
F	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

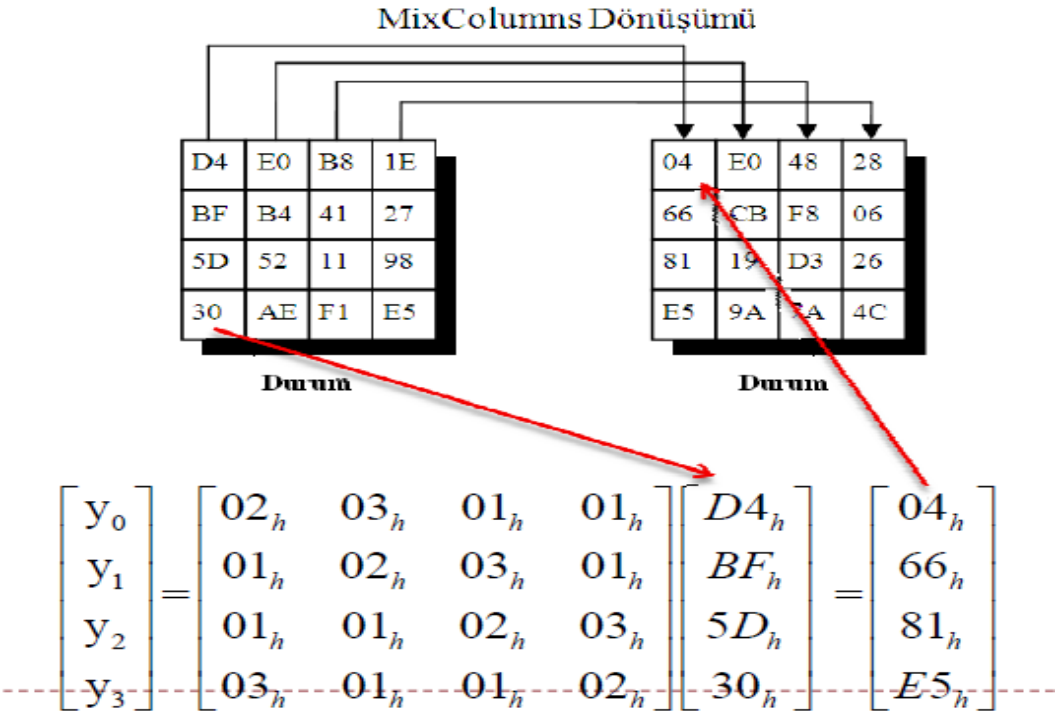
SATIR KAYDIRMA

Satır kaydırma işlemi yeni durum matrisi üzeride yapılır. Bu işlemde matrisin ilk satırı aynı kalırken, ikinci satır 1 bayt, üçüncü satır 2 bayt, dördüncü satır ise 3 bayt sola ötelenir. Bunun sonunda ikinci satırda ilk bayt, üçüncü satırda ilk 2 bayt, dördüncü satırda ilk 3 bayt taar ve bu baytlar da satır sonuna eklenir ve tekrar yeni bir durum matrisi elde edilir.



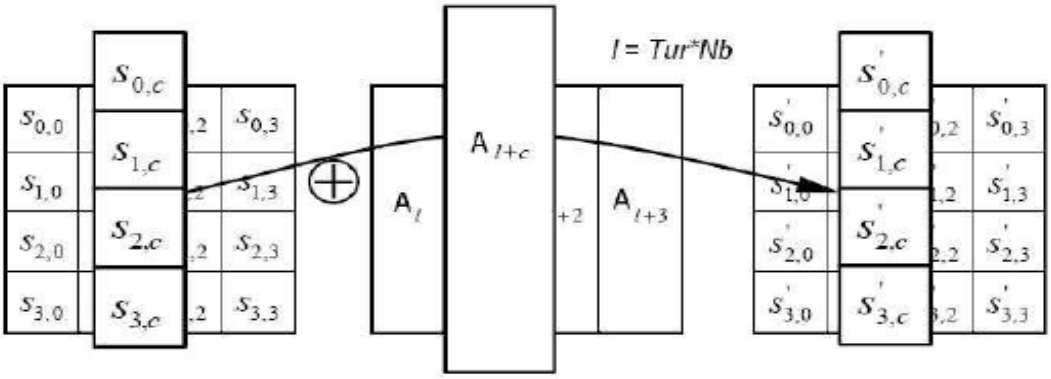
SÜTUN KARIŞTIRMA

Sütunları karıştırma işlemi, satır kaydırmadan elde edilen durum matrisinin her bir sütununu birbirinden bağımsız şekilde $a(x) = \{03\}x^3+\{01\}x^2+\{01\}x+\{02\}$ denklemiyle matris çarpımına tabi tutar. Eski sütunun yerine elde edilen sütun yazılır. Yine durum matrisimiz değişikliğe uğrar. Zaten dönüşüm işlemleri verinin değiştirilmesini hedefler.



DÖNGÜ ANAHTARINI EKLEME

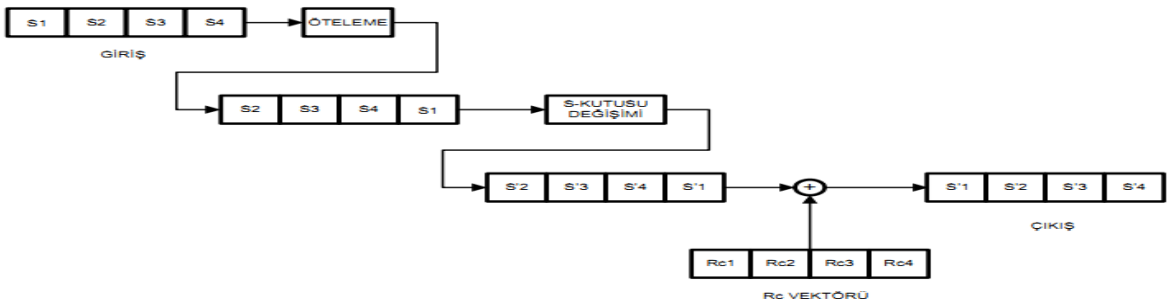
AES algoritmasında her döngünün sonunda anahtar materyali eklenir. Bu anahtar, başlangıçta anahtar üretim bloğu tarafından üretilen anahtar dizisidir. Tur anahtarının uzunluğu blok anahtarının uzunluğuna eşittir(=16bayt). Bu toplama işlemi sonlu alanlarda yapılan her bit için özel veya (XOR) işlemine karşılık düşer.



ANAHTARIN ÜRETİLMESİ

AES algoritmasında anahtar üretme işlemi şifreleme işlemi için önceden yapılması gerekir. Her döngüde farklı bir anahtarın girişi sağlanır. Dolayısıyla anahtar üretme işlemi de döngü sayısı kadar tur içermektedir ve bütün anahtarlar bir önceki turda hesaplanan anahtarların kullanılmasıyla elde edilir.

Anahtar üretim bloğu öncelikle anahtar uzunluğunu bit dizilerinin uzunluğuna göre uygun matrislere çevirir. Tur sayısına: N, matrisin boyutuna: 4xK dersek, daha sonra yapılacak işlemlerle genişlemiş matrisin boyutu 4x(K*(N+1)) olur.



Öncelikle anahtar bitlerinden oluşan matristeki son sütunun(M_4) ilk elemanının sona kaydırılmasıyla başka sütun oluşturulur ve S-Kutusundan bayt değiştirme işlemiyle sütun elemanları değiştirilir.

$\mathbf{M_4}${K1, K2, K3, K4} = $\mathbf{M_4}$ {K2, K3, K4, K1}

{ $\overrightarrow{K2}, \overrightarrow{K3}, \overrightarrow{K4}, \overrightarrow{K1}$ } = S - Kutusu({K2, K3, K4, K1})

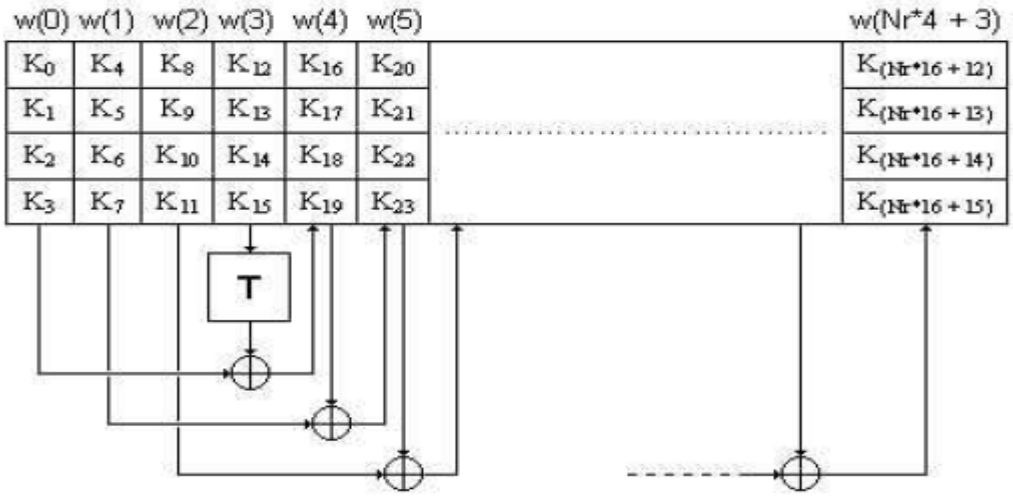
Bu sütun ile ilk sütun(M_1) ve RCON vektör matrisinin 1. sütunun ex-or'lanması işlemi sonucu oluşan yeni sütun, matrise 5. sütun olarak eklenir.

$$\{A1, A2, A3, A4\} = \mathbf{M_1}\{k1, k2, k3, k4\} \oplus \{ \overrightarrow{K2}, \overrightarrow{K3}, \overrightarrow{K4}, \overrightarrow{K1} \} \oplus \{Rcon, 00, 00, 00\}$$

Daha sonra 5. sütun ile 2.sütun ex-or'lanır ve bu yeni sütunda matrise 6. Sütun olarak eklenir. Matrisin her K'nın katı olan sütununa gelince başlangıçtaki ex-or'lanma işlemi yapılır.

$$\mathbf{M_6} = \mathbf{M_5}\{A1, A2, A3, A4\} \oplus \mathbf{M_2}(k1, k2, k3, k4)$$

Bu işlemler tur sayısı kadar devam eder ve matrisin genişlemiş hali elde edilir. Rcon vektörünün hangi sütunun ekleneceği hangi turda olduğuna göre değişiklik gösterir.



Şekil 128 bitlik anahtar bloğunu örneğini gösteriyor. Burada da görüldüğü üzere, anahtar üretimi işleminde oluşan yeni matrisin ilk sütunu hesaplanırken" T işlemi" olarak gösterilen blok ile ayrı bir işlem uygulanır. Diğer sütunlar hesaplanırken, o sütundan bir önceki ve dört önceki sütunlar ex-or işlemine tabi tutulur. Bu işlemler ile 4x4'lük durum matrisi, genişleme sonucu 4x44 boyutunda bir matrise dönüşür. T dediğimiz işlem, öteleme, S kutusundan geçirme ve aşağıdaki tablo da verilen Rcon(i) vektörü ile toplama işleminden oluşan bir işlemler zincirini içermektedir.

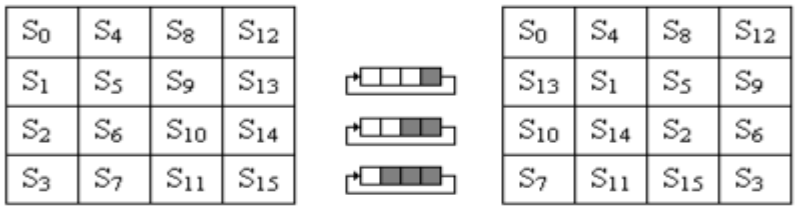
Tur Sayısı	Rcon Değeri	Tur Sayısı	Rcon Değeri
1	**01 00 00 00**	**6**	**20 00 00 00**
2	**02 00 00 00**	**7**	**40 00 00 00**
3	**04 00 00 00**	**8**	**80 00 00 00**
4	**08 00 00 00**	**9**	**1B 00 00 00**
5	**10 00 00 00**	**10**	**36 00 00 00**

ŞİFRE ÇÖZME İŞLEMİ

Rijndael algoritmasında şifreli metni çözmek için uygulanan adımlar şifreleme işlemi için kullanılan adımların benzeridir ve fakat tersi şeklinde uygulanır. Şifrelemek için uygulan dönüşümler tersine çevrilir ve şifreleme sırasının tersinden başlanır. Şifre çözmede Ters sütun kaydırma, Ters bayt yer değiştirme, Ters sütun karıştırma ve Ters tur anahtarı ekleme dönüşümleri kullanılır.

TERS SATIR KAYDIRMA

Ters satır kaydırma işlemi satır kaydırma işleminin tersidir. Bu sefer durum matrisi sola değil sağa doğru kaydırılır. İkinci satır bir bayt, üçüncü satır iki bayt, dördüncü satır üç bayt sağa doğru kaydırılır.



TERS BAYT DEĞİŞTİRME

Şifreleme işleminde bayt değiştirme için bir S-kutusundan yararlanılmıştı. Şifre çözme işleminde de yine aynı şekilde bir S-kutusu kullanılır. Bu S-Kutusu aynı S-Kutusu değildir ve şifreleme için kullanılan kutunu tersidir. Yani 19 değeri S-Kutusunda D4 değerini göstermişti . Şimdiki S-Kutusunda D4'ün 19 değerini göstermesi beklenir. Yani tam tersi bir S-Kutusu kullanılır.

		y														
		0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
x	0	52	09	6a	d5	30	36	a5	38	bf	40	a3	9e	81	f3	d7	fb
	1	7c	e3	39	82	9b	2f	ff	87	34	8e	43	44	c4	de	e9	cb
	2	54	7b	94	32	a6	c2	23	3d	ee	4c	95	0b	42	fa	c3	4e
	3	08	2e	a1	66	28	d9	24	b2	76	5b	a2	49	6d	8b	d1	25
	4	72	f8	f6	64	86	68	98	16	d4	a4	5c	cc	5d	65	b6	92
	5	6c	70	48	50	fd	ed	b9	da	5e	15	46	57	a7	8d	9d	84
	6	90	d8	ab	00	8c	bc	d3	0a	f7	e4	58	05	b8	b3	45	06
	7	d0	2c	1e	8f	ca	3f	0f	02	c1	af	bd	03	01	13	8a	6b
	8	3a	91	11	41	4f	67	dc	ea	97	f2	cf	ce	f0	b4	e6	73
	9	96	ac	74	22	e7	ad	35	85	e2	f9	37	e8	1c	75	df	6e
	a	47	f1	1a	71	1d	29	c5	89	6f	b7	62	0e	aa	18	be	1b
	b	fc	56	3e	4b	c6	d2	79	20	9a	db	c0	fe	78	cd	5a	f4
	c	1f	dd	a8	33	88	07	c7	31	b1	12	10	59	27	80	ec	5f
	d	60	51	7f	a9	19	b5	4a	0d	2d	e5	7a	9f	93	c9	9c	ef
	e	a0	e0	3b	4d	ae	2a	f5	b0	c8	eb	bb	3c	83	53	99	61
	f	17	2b	04	7e	ba	77	d6	26	e1	69	14	63	55	21	0c	7d

TERS SÜTUN DEĞİŞTİRME

Ters sütun değiştirmede şifrelemedeki sütun değiştirme mantığı ile aynıdır. Yine her sütun bir polinom ile çarpılır ve elde edile yeni sütun eskisinin yerine yazılır. Fakat buradaki matris çarpımında kullanılan polinom farklıdır. Durum matrisinin her sütunu $GF(2^8)$ sonlu alanında tanımlı dört terimli bir polinomlar olarak düşünülür.

$a^{-1}(x) = \{0B\}x^3 + \{0D\}x^2 + \{09\}x + \{0E\}$

$s'(x) = a^{-1}(x) \otimes s(x)$

ile ifade edildiğinde, bu işlem aşağıda bulunan şekildeki gibi matris çarpması halinde gösterilebilir.

$$\begin{bmatrix} s'_{0,c} \\ s'_{1,c} \\ s'_{2,c} \\ s'_{3,c} \end{bmatrix} = \begin{bmatrix} 0e & 0b & 0d & 09 \\ 09 & 0e & 0b & 0d \\ 0d & 09 & 0e & 0b \\ 0b & 0d & 09 & 0e \end{bmatrix} \begin{bmatrix} s_{0,c} \\ s_{1,c} \\ s_{2,c} \\ s_{3,c} \end{bmatrix}$$

ÇÖZME İŞLEMİNDE DÖNGÜ ANAHTARINI EKLEME

Döngü anahtarını eklemenin tersi yine kendisidir. Aes algoritması şifreleme ve şifreyi çözmede aynı anahtarı kullanan simetrik yapıya sahiptir. Aynı anahtarı kullanmak demek anahtar üretme bloğunda yürütülen matris genişleme işlemlerinin girişine aynı matrisin geleceği demektir. Genişletilen matriste üretilen matrisler aynı olacağından şifre çözme içi yapılan döngünün sonunda eklenen anahtar materyalleri de aynısı olur.