Bilgi Güvenliği ve Kriptografi

AES (Advanced Encryption Standard)

- Kriptografi uzmanları olan Joan Daemen ve Vincent Rijmen tarafından geliştirilmiş

  128-bitlik,

  192-bitlik,

  256-bitlik

anahtar uzunluğu seçeneklerine sahip olan Rijndael algoritması,

Gelişmiş Şifreleme Standardı (AES) ismiyle elektronik ortamda veri güvenliğini sağlanması amacıyla veri şifreleme standardı olarak kabul edilmiştir.

AES (Advanced Encryption Standard)

- 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.

AES (Advanced Encryption Standard)

- Rijndael algoritması, sahip olduğu anahtarlara göre farklı sayıda döngüsel işlemler yapar.
- Her döngü sonunda anahtar yenilenir ve veriye uygulanır.
- Veri öncelikle diziler şeklinde ifade edilir.
- AES 128-bitlik düz metni şifrelerken ve 128-bitlik şifrelenmiş metni çözerken de aynı anahtarı kullanır.

AES (Advanced Encryption Standard)

- 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 adlandırılır.
- AES şifrelerken kullanacağı algoritmada anahtarın uzunluğuna göre döngü sayısının atamasını yapar. Bu döngüsel işlemin artmasıyla veri daha güvenilir hale gelir.
- Fakat yapılacak olan döngüsel işlemlerin artmasıyla hem işlem sayısı artar hem de bellek alanı artar.

AES (Advanced Encryption Standard)

- Şifrelemeyi oluşturacak anahtar da aynı zamanda durum dediğimiz matris formuna 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

AES (Advanced Encryption Standard)

- AES algoritmasının en küçük parçası, durum matrisinin elemanı 8-bitlik diziden oluşan bayttır.
- Şifrelenecek metin, şifreleme anahtarı ve şifrelenmiş metin, baytlar haline dönüştürülür ve bunların birleşiminden bayt dizileri oluşur.
- Bu bayt dizilerinin uzunluğu, şifreleme anahtarının uzunluğuna göre doğrusal olarak değişir. Böylece matris boyutu da değişmiş olur.
- 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 (Advanced Encryption Standard)

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.

$(0000)_2=(0)_{16}$	$(1000)_2=(8)_{16}$
$(0001)_2=(1)_{16}$	$(1001)_2=(9)_{16}$
$(0010)_2=(2)_{16}$	$(1010)_2=(A)_{16}$
$(0011)_2=(3)_{16}$	$(1011)_2=(B)_{16}$
$(0100)_2=(4)_{16}$	$(1100)_2=(C)_{16}$
$(0101)_2=(5)_{16}$	$(1101)_2=(D)_{16}$
$(0110)_2=(6)_{16}$	$(1110)_2=(E)_{16}$
$(0111)_2=(7)_{16}$	$(1111)_2=(F)_{16}$

AES (Advanced Encryption Standard)

- Bayt değerlerini onaltılık tabanda göstermek mümkündür. İlk dört bit ve son dört bit birer hexadecimal karakterle gösterilir
- **"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**

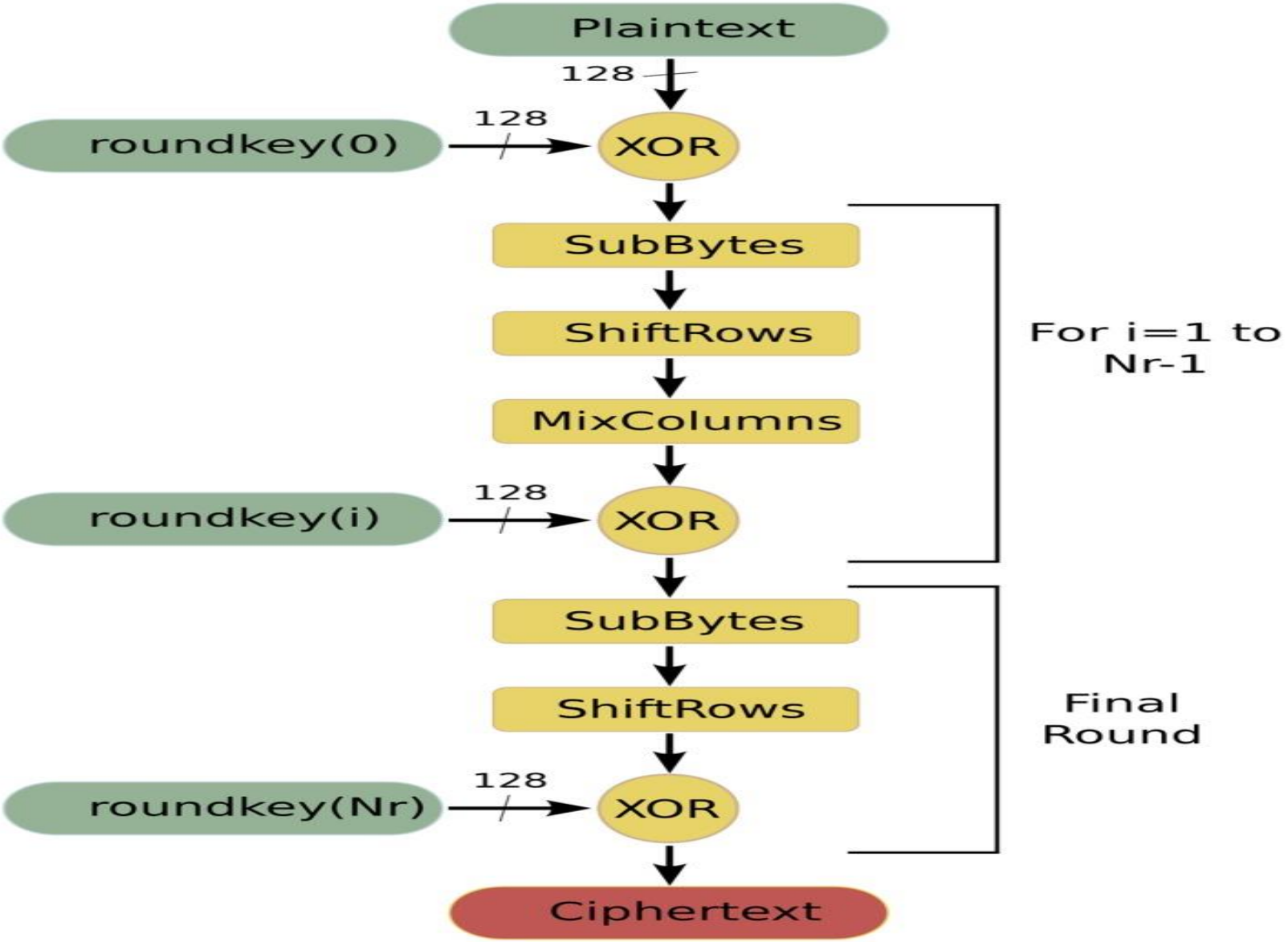
AES (Advanced Encryption Standard)

- 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.

AES (Advanced Encryption Standard)

- Döngüler durum matrislerinde 4 dönüşüm uygular.
  - *BaytDeğiştir (SubBytes)* - Durum matrisindeki her bayt bir tabloya göre ve doğrusal olmayan bir dönüşümle güncellenir.
  - *SatırKaydır (ShiftRows)* - Her satır belirli bir sayıda diresel olarak kaydırılır.
  - *SütunKarıştır (MixColumn)* - Her bir sütundaki dört bayt, birbiriyle karıştırılır.
  - *AnahtarEkle (AddRoundKey)* - Durum matrisi, ilk çevrim anahtarı ile XOR'lanır.
- Her döngüde işleme farklı anahtar sokulur. Bu farklı anahtarlar, başlangıçta belirlenen anahtardan üretilirler.

AES (Advanced Encryption Standard)

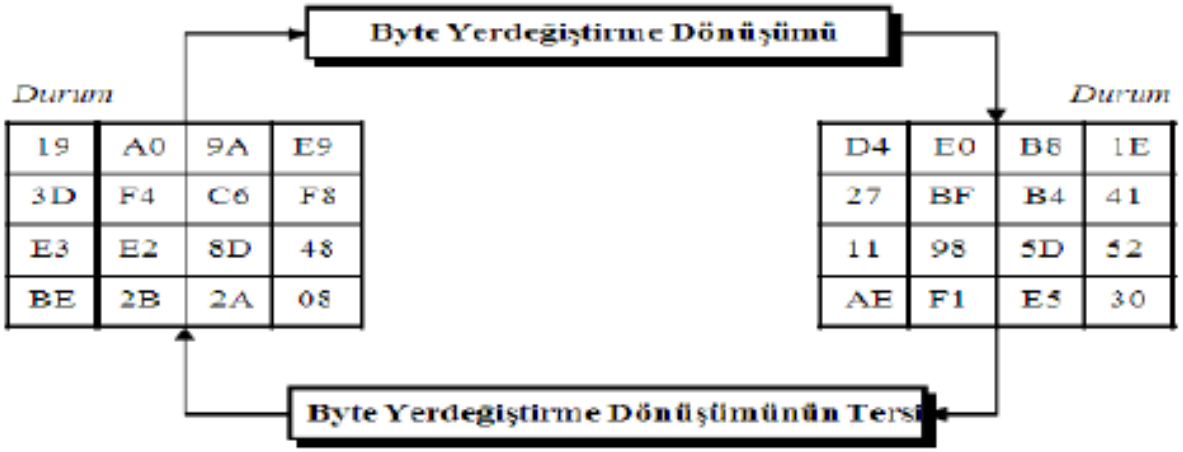


AES (Advanced Encryption Standard)

Bayt Değiştirme

- 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.
- 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.

AES (Advanced Encryption Standard)



	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

AES (Advanced Encryption Standard)

- Örneğin 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 S-Kutusunda D4'tür.

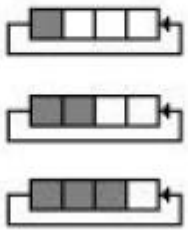
- Bu işlem matrisin tüm elemanlarına uygulanır ve yeni bir durum matrisi elde edilir.

AES (Advanced Encryption Standard)

Satır Kaydırma

- Satır kaydırma işlemi yeni durum matrisi üzerinde 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 taşar ve bu baytlar da satır sonuna eklenir ve tekrar yeni bir durum matrisi elde edilir.

S_0	S_4	S_8	S_{12}
S_1	S_5	S_9	S_{13}
S_2	S_6	S_{10}	S_{14}
S_3	S_7	S_{11}	S_{15}

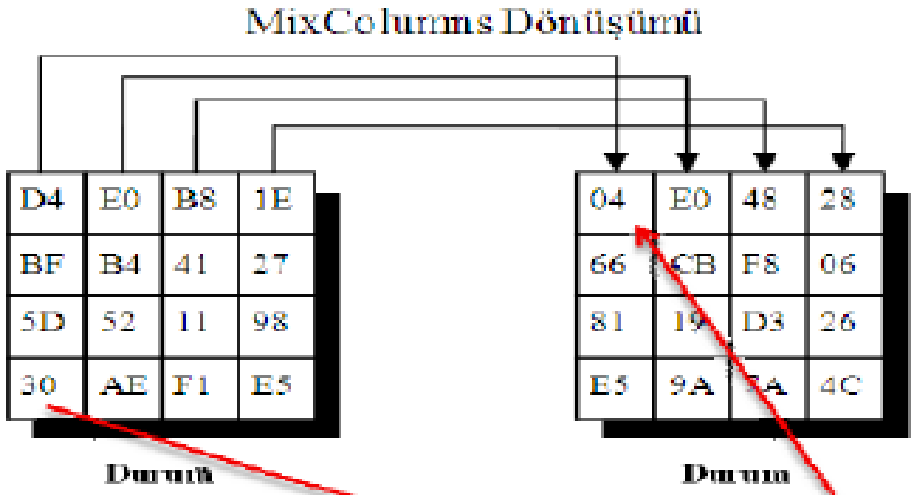


S_0	S_4	S_8	S_{12}
S_5	S_9	S_{13}	S_1
S_{10}	S_{14}	S_2	S_6
S_{15}	S_3	S_7	S_{11}

AES (Advanced Encryption Standard)

Sütün Karıştırma

- Sütunları karıştırma işlemi, satır kaydırmadan elde edilen durum matrisinin her bir sütununu birbirinden bağımsız matris çarpımına tabi tutar. Eski sütunun yerine elde edilen sütun yazılır.

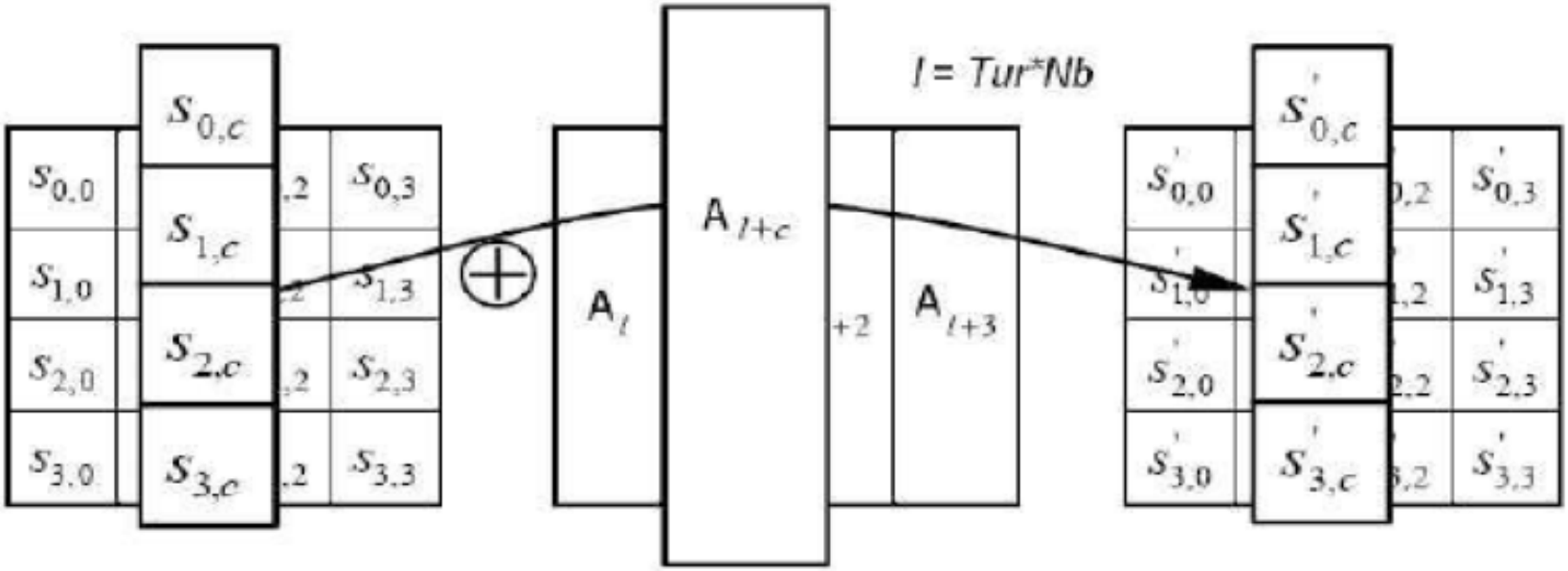


$$\begin{bmatrix} y_0 \\ y_1 \\ y_2 \\ y_3 \end{bmatrix} = \begin{bmatrix} 02_h & 03_h & 01_h & 01_h \\ 01_h & 02_h & 03_h & 01_h \\ 01_h & 01_h & 02_h & 03_h \\ 03_h & 01_h & 01_h & 02_h \end{bmatrix} \begin{bmatrix} D4_h \\ BF_h \\ 5D_h \\ 30_h \end{bmatrix} = \begin{bmatrix} 04_h \\ 66_h \\ 81_h \\ E5_h \end{bmatrix}$$

AES (Advanced Encryption Standard)

Anahtar Ekleme

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



AES (Advanced Encryption Standard)

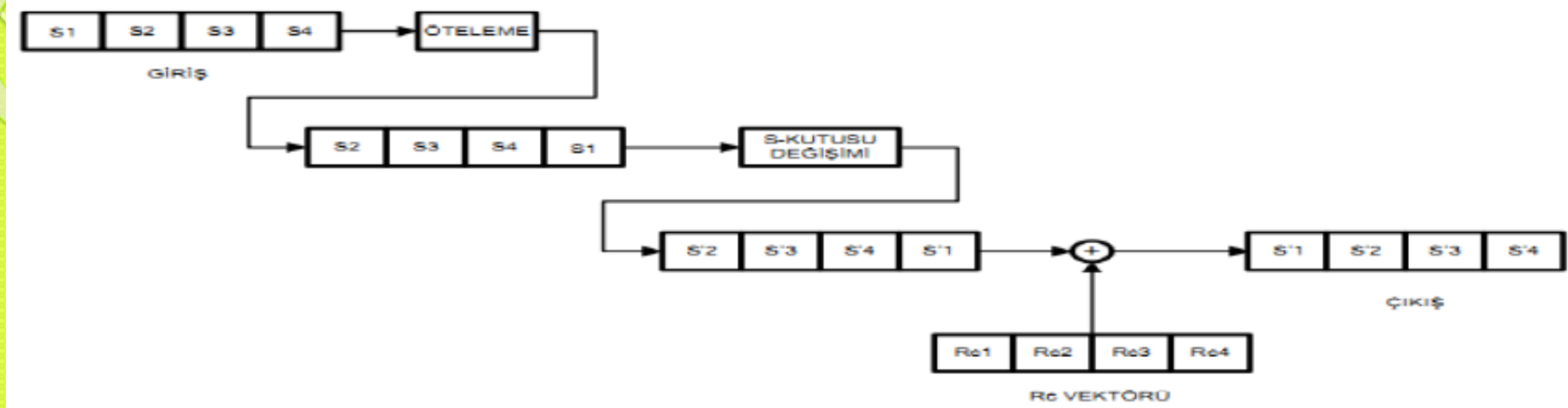
Anahtar Üretimi

- AES algoritmasında anahtar üretme işleminin şifreleme işleminden önce 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.

AES (Advanced Encryption Standard)



- Öncelikle anahtar bitlerinden oluşan matristeki son sütunun(M4) ilk elemanının sona kaydırılmasıyla başka sütun oluşturulur ve S-Kutusundan bayt değiştirme işlemiyle sütun elemanları değiştirilir.

$$\mathbf{M}_4\{K1, K2, K3, K4\} = \mathbf{M}_4\{K2, K3, K4, K1\}$$

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

AES (Advanced Encryption Standard)

- Bu sütun ile ilk sütun(M1) ve RCON vektör matrisinin 1. sütunun XOR'lanması işlemi sonucu oluşan yeni sütun, matrise 5. sütun olarak eklenir.

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

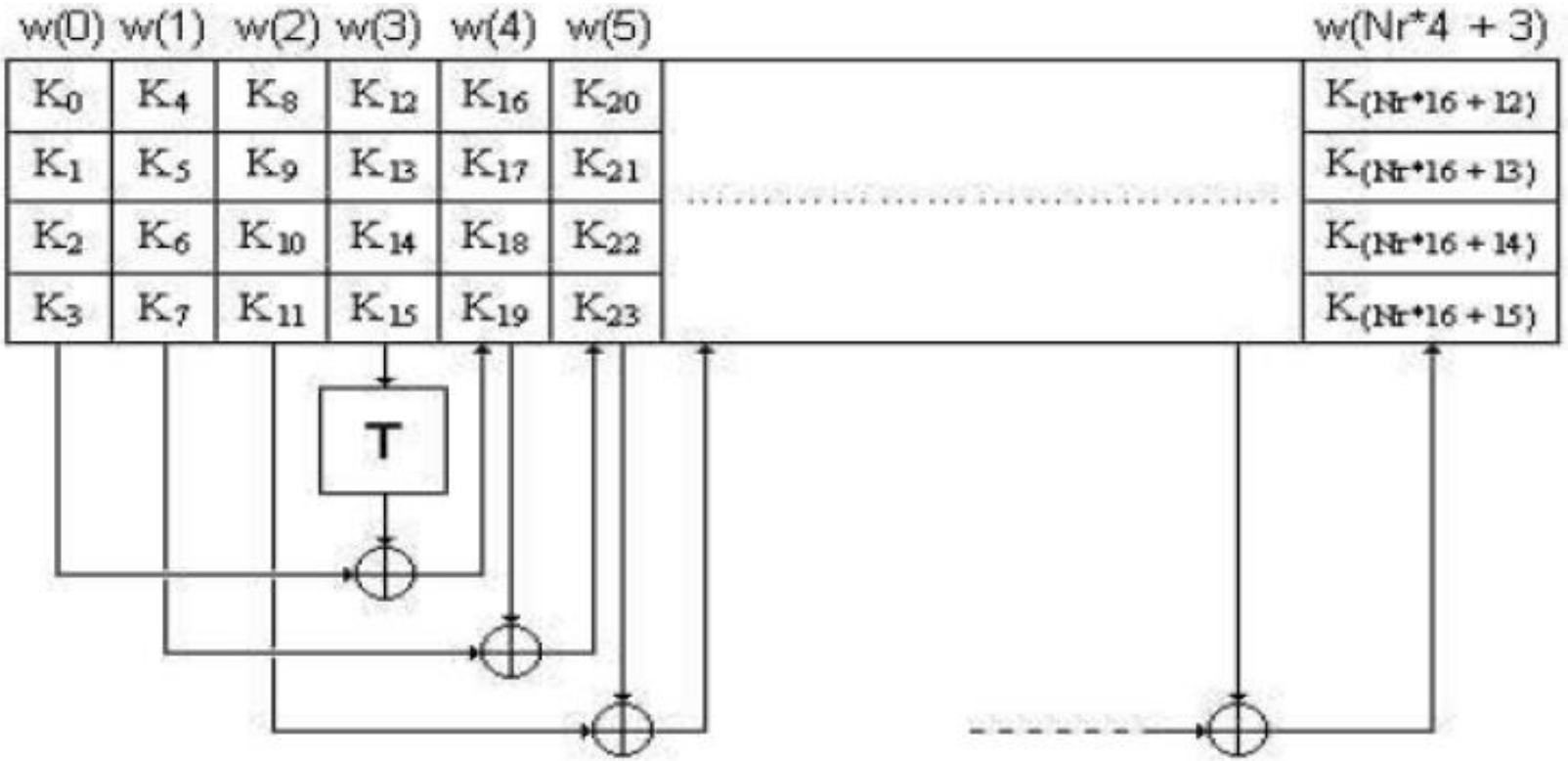
- Daha sonra 5. sütun ile 2.sütun XOR'lanır ve bu yeni sütunda matrise 6. Sütun olarak eklenir. Matrisin her K'nın katı olan sütununa gelince başlangıçtaki XOR'lanma işlemi yapılır.

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

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

AES (Advanced Encryption Standard)

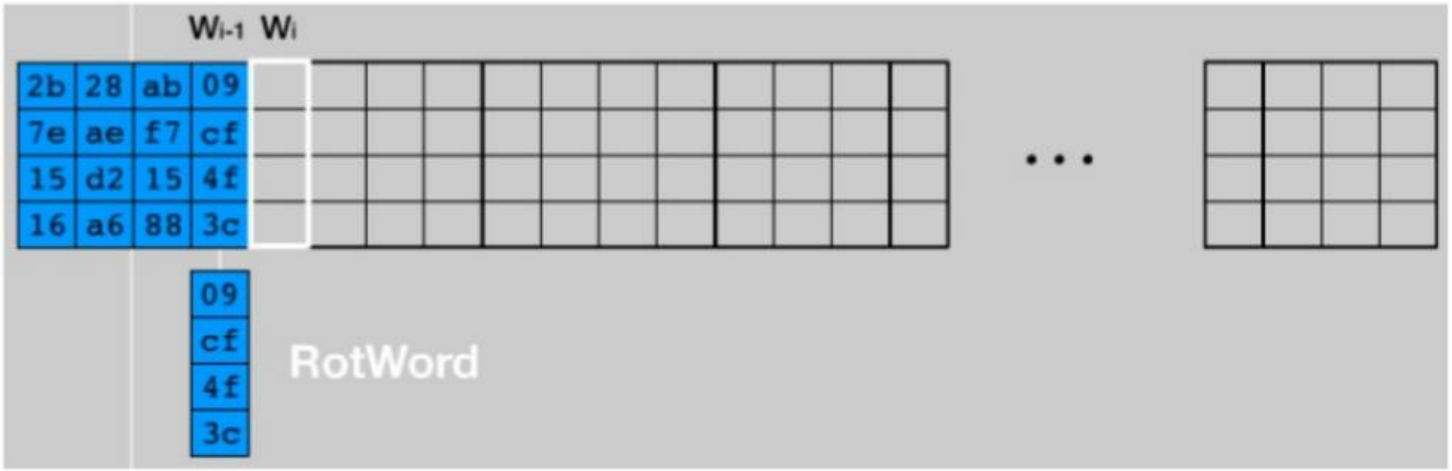
Tur Sayısı	Rcon Değeri	Tur Sayısı	Rcon Değeri
1	01 00 00 00	6	20 00 00 00
2	02 00 00 00	7	40 00 00 00
3	04 00 00 00	8	80 00 00 00
4	08 00 00 00	9	1B 00 00 00
5	10 00 00 00	10	36 00 00 00

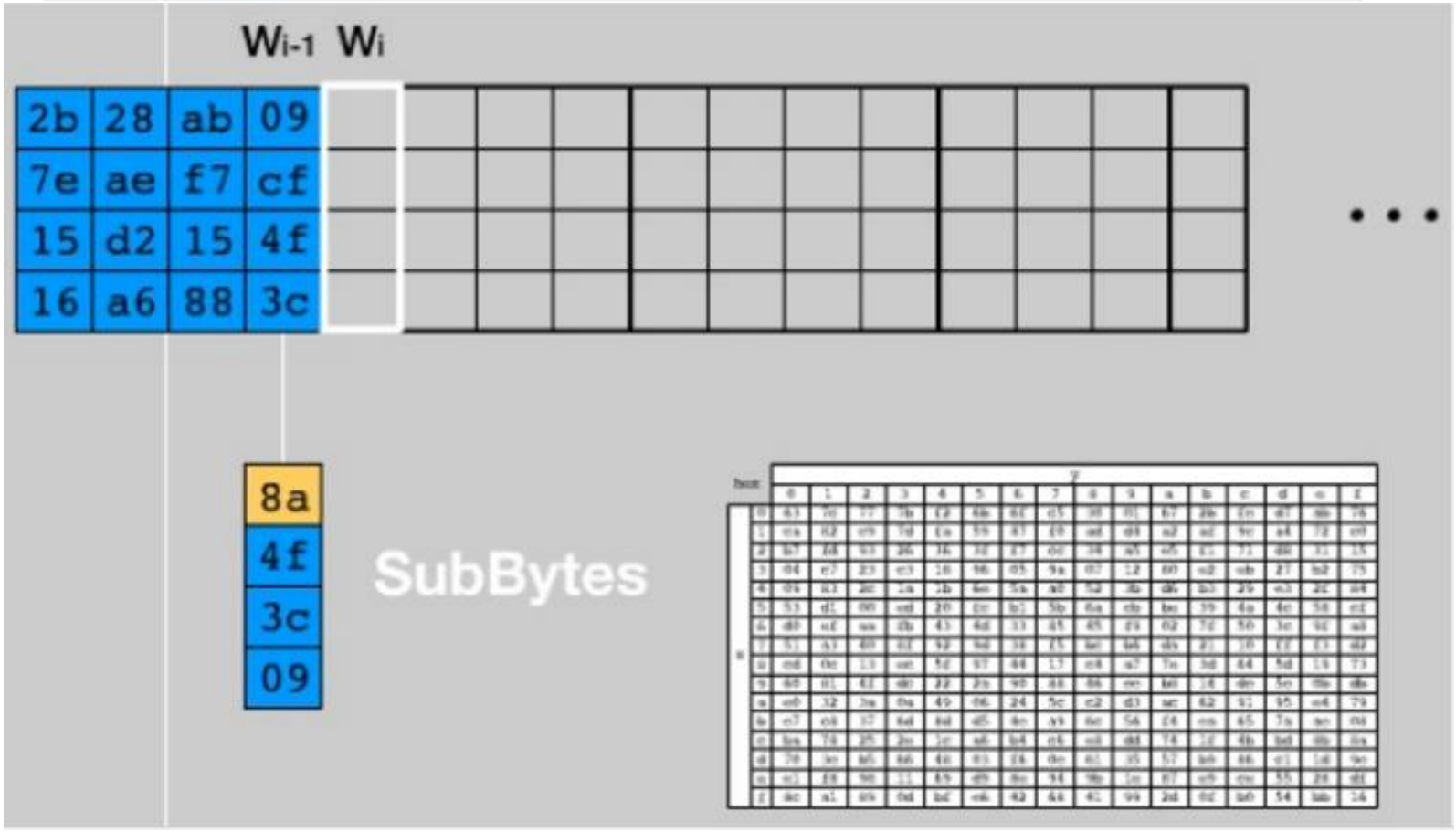


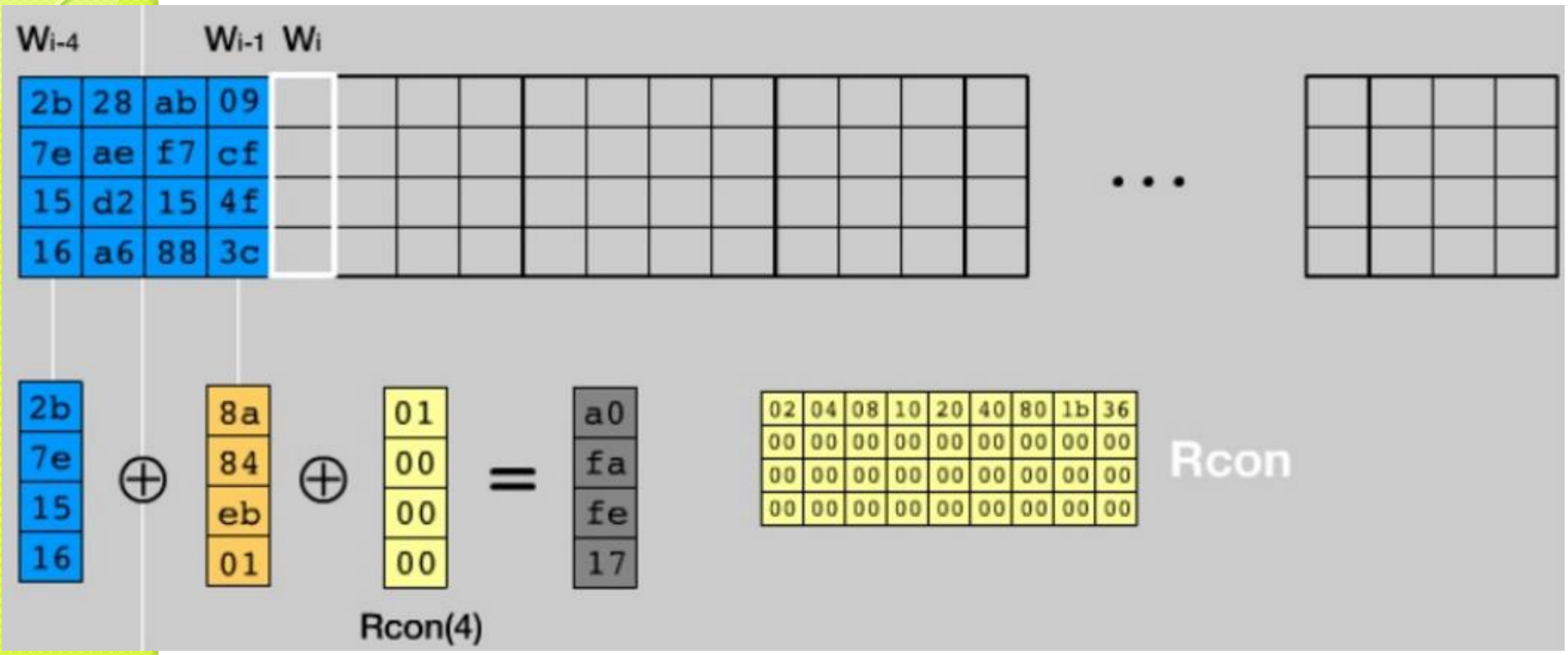
AES (Advanced Encryption Standard)

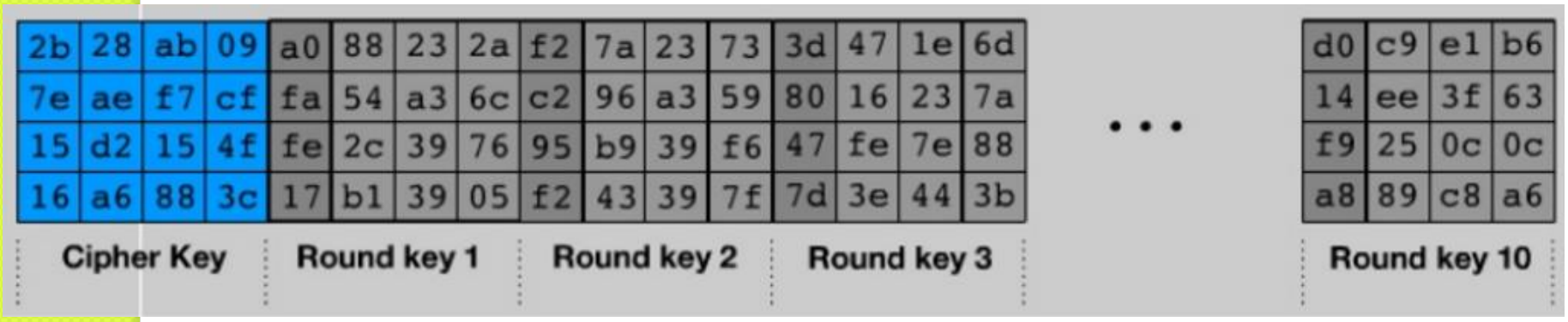
- Şekil 128 bitlik anahtar bloğu örneğini gösteriyor. Burada da görüldüğü üzere, anahtar üretimi işleminde oluşan yeni matrisin ilk sütunu hesaplanırken“ T işlemi” olarak gösterilen blok ile ayrı bir işlem uygulanır. Diğer sütunlar hesaplanırken, o sütundan bir önceki ve dört önceki sütunlar XOR işlemine tabi tutulur. Bu işlemler ile 4x4'lük durum matrisi, genişleme sonucu 4x44 boyutunda bir matrise dönüşür.

- T dediğimiz işlem, öteleme, S kutusundan geçirme ve tablo da verilen Rcon(i) vektörü ile toplama işleminden oluşan bir işlemler zincirini içermektedir.


Wi-1 Wi
2b 28 ab 09
7e ae f7 cf
15 d2 15 4f
16 a6 88 3c
09
cf
4f
3c
RotWord


Wi-1 Wi
2b 28 ab 09
7e ae f7 cf
15 d2 15 4f
16 a6 88 3c
8a
4f
3c
09
SubBytes


Wi-4
Wi-1
Wi
2b 28 ab 09
7e ae f7 cf
15 d2 15 4f
16 a6 88 3c
2b
7e
15
16
8a
84
eb
01
01
00
00
00
Rcon(4)
a0
fa
fe
17
02 04 08 10 20 40 80 1b 36
00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00
Rcon


2b 28 ab 09 a0 88 23 2a f2 7a 23 73 3d 47 1e 6d
7e ae f7 cf fa 54 a3 6c c2 96 a3 59 80 16 23 7a
15 d2 15 4f fe 2c 39 76 95 b9 39 f6 47 fe 7e 88
16 a6 88 3c 17 b1 39 05 f2 43 39 7f 7d 3e 44 3b
d0 c9 e1 b6
14 ee 3f 63
f9 25 0c 0c
a8 89 c8 a6
Cipher Key
Round key 1
Round key 2
Round key 3
Round key 10