CS557: Cryptography

Modern Ciphers (AES)

S. Tripathy
IIT Patna

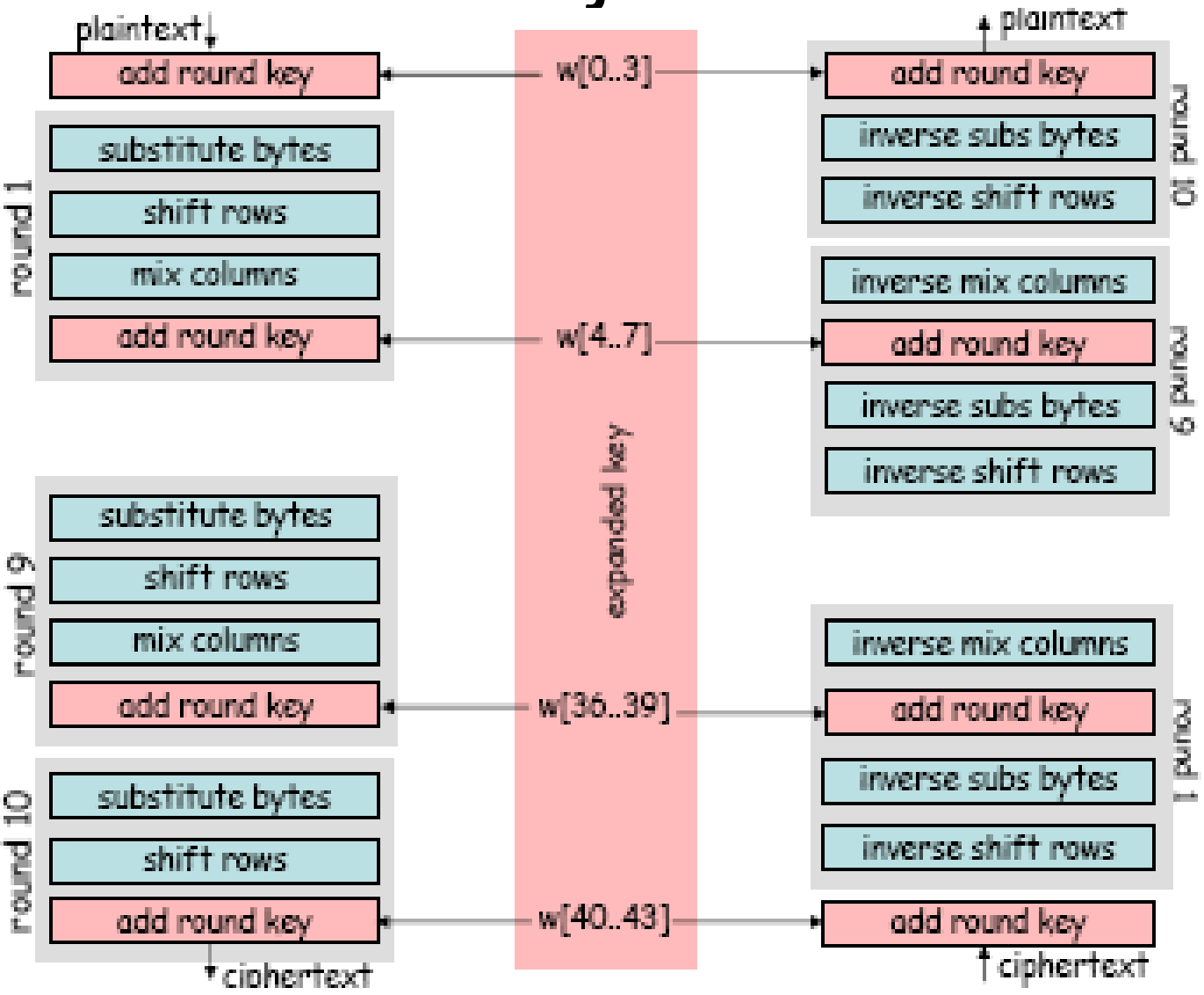
AES

- AES-Rijndael parameters
  - key size 128/ 192/ 256/ -bit
  - input/output size 128-bit
  - number of rounds 10 12 14
  - round key size 128

- **Decryption algorithm is different from encryption algorithm (non Feistel structure). (optimized for encryption)**

- single 8 bit to 8 bit S-box.
- stronger & faster than Triple-DES

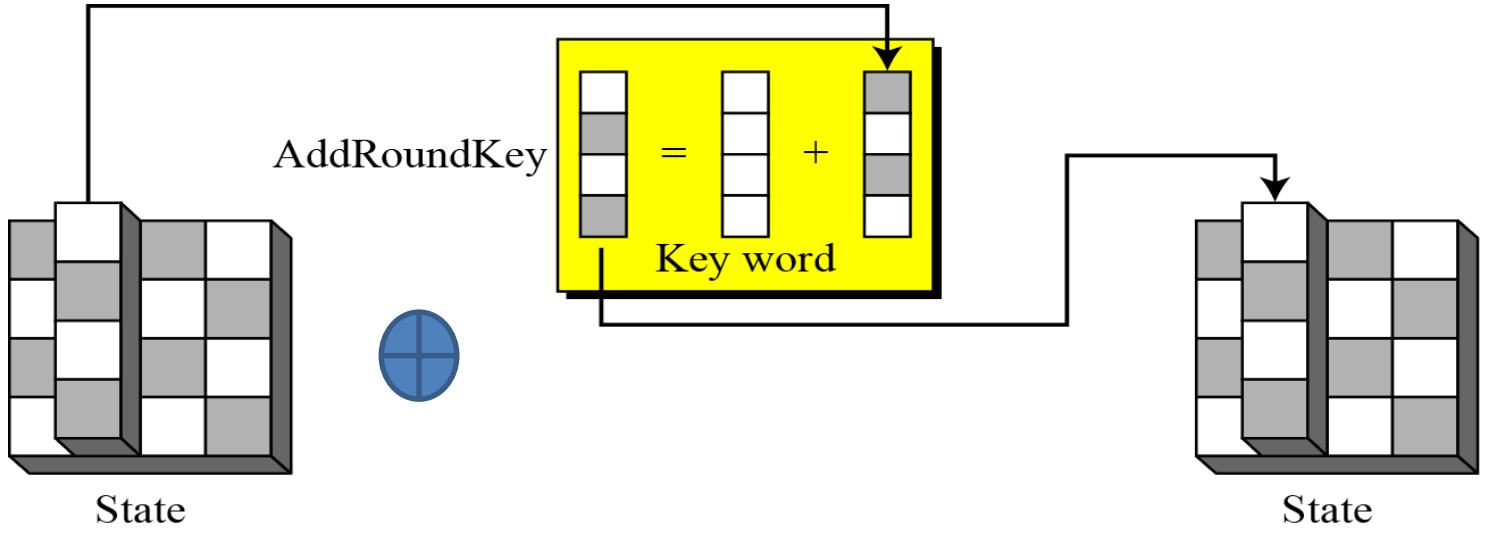
AES-Rijndael



AES Round Function Components:

Add Round Key

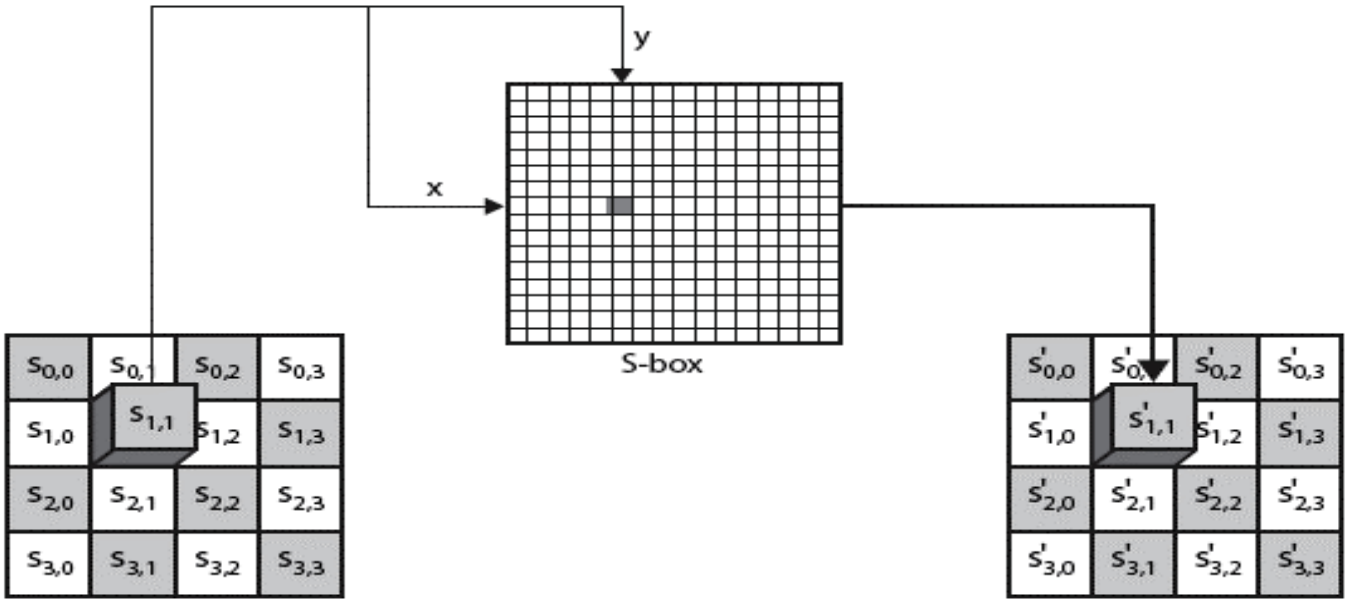
- AddRoundKey proceeds one column at a time.
- AddRoundKey adds a round key word with each state column matrix; the operation in AddRoundKey is matrix addition



AES Round Function Components:

Byte Substitution

- uses one table of 16x16 bytes containing a permutation of all 256 8-bit values
- each byte of state is replaced by byte in row (left 4-bits) & column (right 4-bits)
  - eg. $S_{1,1}$ byte {4E} is replaced by row 4 col E byte (in S-Table)
  - which is the value $S_{1,1}$'{2F}



S-box

		y															
		0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
x	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

S-Box Byte Computation

S-box is constructed defined transformation of the values in GF(2^8) with irreducible polynomial ($x^8 + x^4 + x^3 + x + 1$) as $y = Ax^{-1} + c$

$$\begin{bmatrix} s_0 \\ s_1 \\ s_2 \\ s_3 \\ s_4 \\ s_5 \\ s_6 \\ s_7 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \\ b_6 \\ b_7 \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix}$$

Ex.: X = 0x11, X^{-1} = 0xb4 = (10110100), $A X^{-1} + C = 82$

$$s = b \oplus (b \lll 1) \oplus (b \lll 2) \oplus (b \lll 3) \oplus (b \lll 4) \oplus 63_{16}$$

$$s_i = b_i \oplus b_{(i+4) \bmod 8} \oplus b_{(i+5) \bmod 8} \oplus b_{(i+6) \bmod 8} \oplus b_{(i+7) \bmod 8} \oplus c_i$$

AES Round Function Components:

Shift Rows

A:

sij is a byte

s00	s01	s02	s03
s10	s11	s12	s13
s20	s21	s22	s23
s30	s31	s32	s33

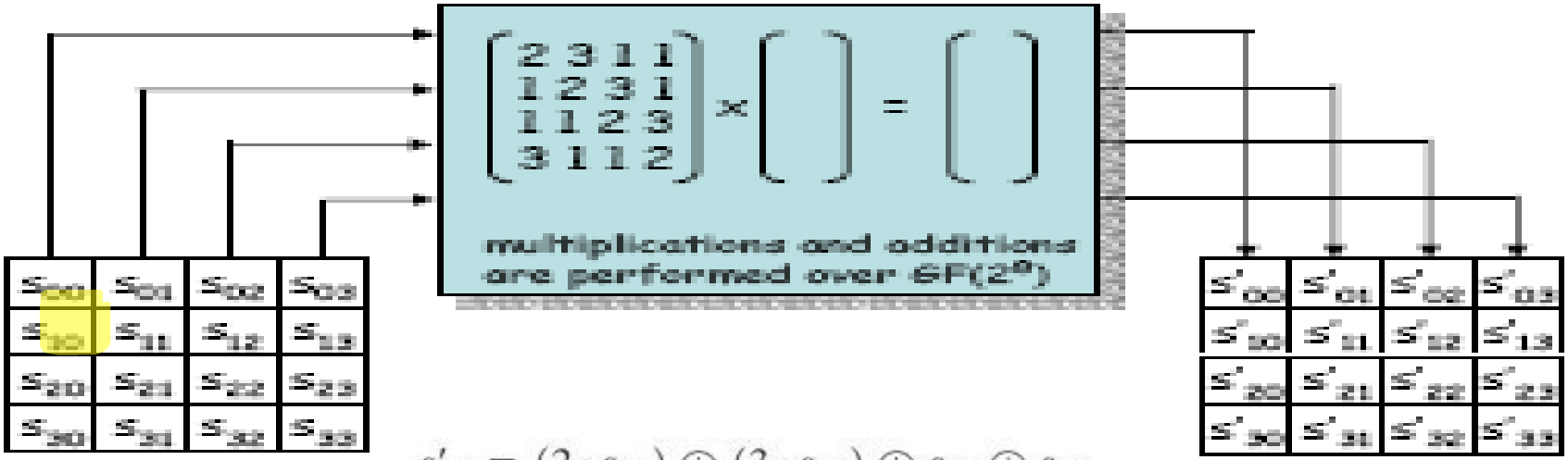
Shift row i
i positions
(i = 0 to 3)

s00	s01	s02	s03
s11	s12	s13	s10
s22	s23	s20	s21
s33	s30	s31	s32

AES Round Function Components:

Mix Columns

- Each column is multiplied modulo (x^4+1) by the fixed polynomial a(x), given by
  $a(x) = \{03\}x^3 + \{01\}x^2 + \{01\}x + \{02\}$
- effectively a matrix multiplication in GF(2^8) using prime poly $m(x) = x^8+x^4+x^3+x+1$



$$s'_{0,j} = (2 \bullet s_{0,j}) \oplus (3 \bullet s_{1,j}) \oplus s_{2,j} \oplus s_{3,j}$$
$$s'_{1,j} = s_{0,j} \oplus (2 \bullet s_{1,j}) \oplus (3 \bullet s_{2,j}) \oplus s_{3,j}$$
$$s'_{2,j} = s_{0,j} \oplus s_{1,j} \oplus (2 \bullet s_{2,j}) \oplus (3 \bullet s_{3,j})$$
$$s'_{3,j} = (3 \bullet s_{0,j}) \oplus s_{1,j} \oplus s_{2,j} \oplus (2 \bullet s_{3,j})$$

AES Decryption

- **The AES Decryption Algorithm:**

❑ **AddRoundKey:**

- Add Roundkey transformation is identical to the forward add round key transformation, because the XOR operation is its own inverse.

$$A \leftarrow \text{round\_key} \oplus A$$

❑ **Inverse SubBytes:**

- This operation can be performed using the inverse S-Box. It is read identically to the S-Box matrix.

❑ **InvShiftRows:**

- Inverse Shift Ro… …cular shifts in… for each of the … …a one-byte ci… the second row, …

s00	s01	s02	s03
s10	s11	s12	s13
s20	s21	s22	s23
s30	s31	s32	s33

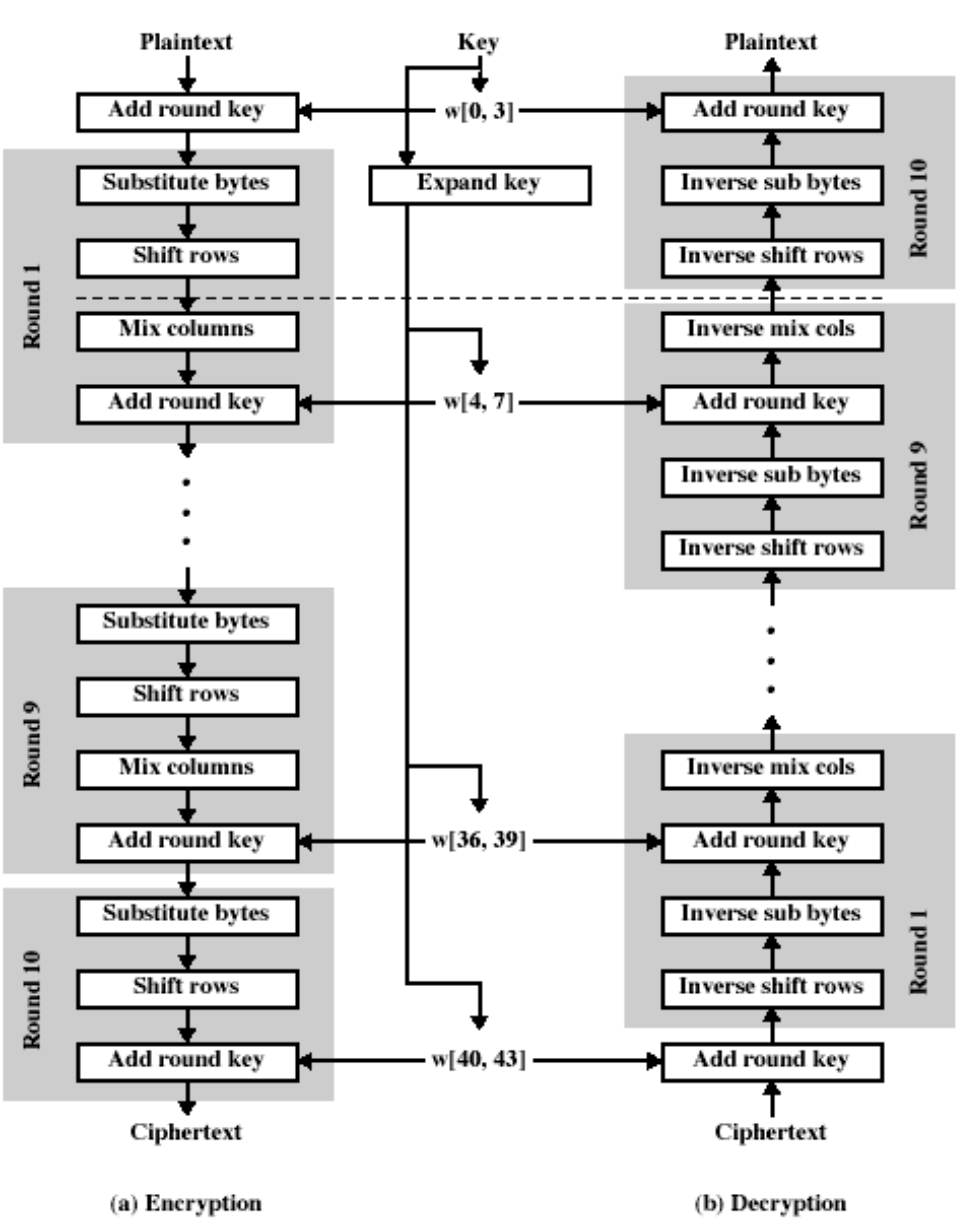
Shift row i
i positions
(i = 0 to 3)

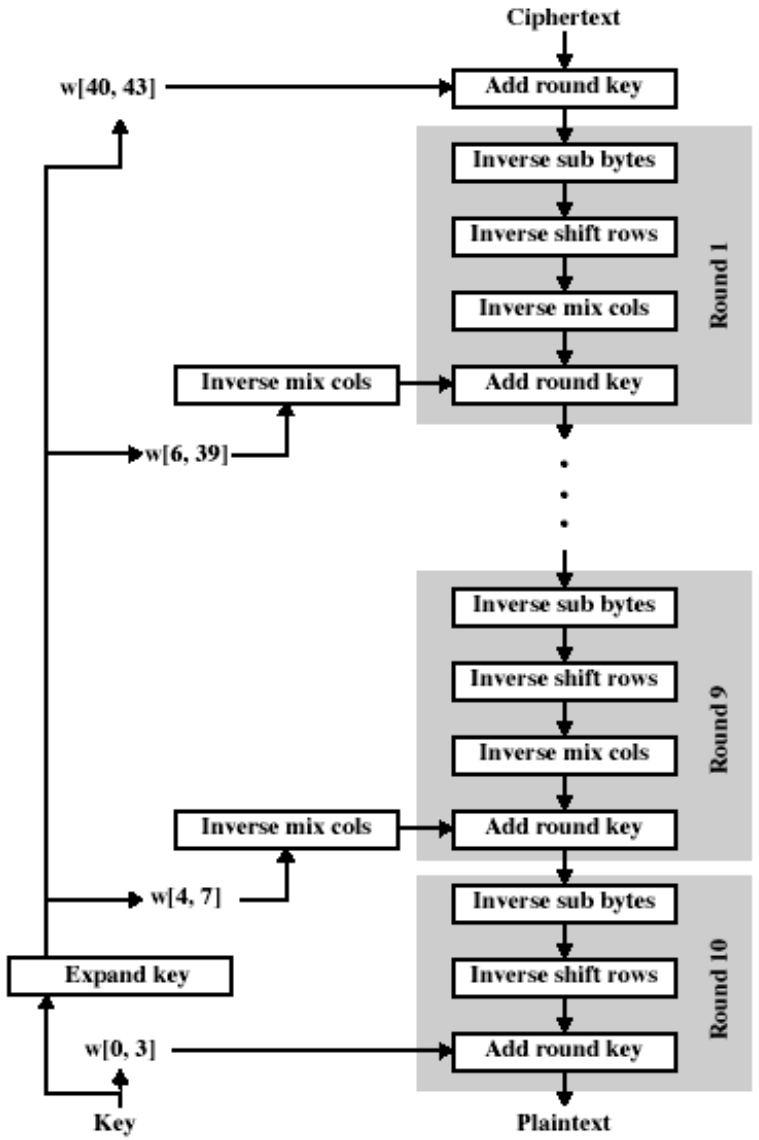
s00	s01	s02	s03
s11	s12	s13	s10
s22	s23	s20	s21
s33	s30	s31	s32

❑ **InvMixColumns:**

$$A \leftarrow \begin{matrix} 0E & 0B & 0D & 09 \\ 09 & 0E & 0B & 0D \\ 0D & 09 & 0E & 0B \\ 0B & 0D & 09 & 0E \end{matrix} * A$$

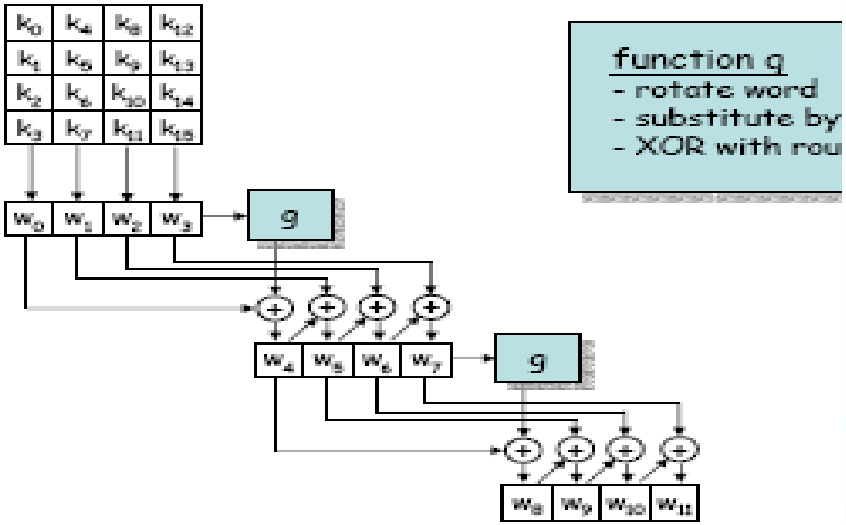
- The inverse mix column transformation is … …he following matrix multiplication in Galois Field (2^8):


Plaintext
Key
Add round key
w[0, 3]
Substitute bytes
Expand key
Shift rows
Round 1
Mix columns
Add round key
w[4, 7]
Substitute bytes
Shift rows
Round 9
Mix columns
Add round key
w[36, 39]
Substitute bytes
Shift rows
Round 10
Add round key
w[40, 43]
Ciphertext
(a) Encryption
Plaintext
Add round key
Inverse sub bytes
Inverse shift rows
Round 10
Inverse mix cols
Add round key
Inverse sub bytes
Inverse shift rows
Round 9
Inverse mix cols
Add round key
Inverse sub bytes
Inverse shift rows
Round 1
Add round key
Ciphertext
(b) Decryption


Ciphertext
w[40, 43]
Add round key
Inverse sub bytes
Inverse shift rows
Inverse mix cols
Round 1
Inverse mix cols
Add round key
w[6, 39]
Inverse sub bytes
Inverse shift rows
Inverse mix cols
Round 9
Inverse mix cols
Add round key
w[4, 7]
Inverse sub bytes
Inverse shift rows
Round 10
Expand key
w[0, 3]
Add round key
Key
Plaintext

AES Key Expansion

- takes 128/192/256-bit (16/24/32-byte) key and expands into array of 44/52/60 32-bit words
- start by copying key into first 4 words
- then loop creating words that depend on values in previous and 4 places back
  - in 3 of 4 cases just XOR these together
  - every 4th has S-box + rotate + XO



function g
- rotate word
- substitute by
- XOR with rou

Key Words	Auxiliary Function
w0 = 0f 15 71 c9	RotWord(w3)= 7f 67 98 af = x1
w1 = 47 d9 e8 59	SubWord(x1)= d2 85 46 79 = y1
w2 = 0c b7 ad	Rcon(1)= 01 00 00 00
w3 = af 7f 67 98	y1 ⊕ Rcon(1)= d3 85 46 79 = z1
w4 = w0 ⊕ z1 = dc 90 37 b0	RotWord(w7)= 81 15 a7 38 = x2
w5 = w4 ⊕ w1 = 9b 49 df e9	SubWord(x4)= 0c 59 5c 07 = y2
w6 = w5 ⊕ w2 = 97 fe 72 3f	Rcon(2)= 02 00 00 00
w7 = w6 ⊕ w3 = 38 81 15 a7	y2 ⊕ Rcon(2)= 0e 59 5c 07 = z2
w8 = w4 ⊕ z2 = d2 c9 6b b7	RotWord(w11)= ff d3 c6 e6 = x3
w9 = w8 ⊕ w5 = 49 80 b4 5e	SubWord(x2)= 16 66 b4 8e = y3
w10 = w9 ⊕ w6 = de 7e c6 61	Rcon(3)= 04 00 00 00
w11 = w10 ⊕ w7 = e6 ff d3 c6	y3 ⊕ Rcon(3)= 12 66 b4 8e = z3
w12 = w8 ⊕ z3 = c0 af df 39	RotWord(w15)= ae 7e c0 b1 = x4
w13 = w12 ⊕ w9 = 89 2f 6b 67	SubWord(x3)= e4 f3 ba c8 = y4
w14 = w13 ⊕ w10 = 57 51 ad 06	Rcon(4)= 08 00 00 00
w15 = w14 ⊕ w11 = b1 ae 7e c0	y4 ⊕ Rcon(4)= ec f3 ba c8 = 4

AES Diffusion: Single Byte

Round 1

s00	s01	s02	s03
s10	s11	s12	s13
s20	s21	s22	s23
s30	s31	s32	s33

Input

s00	s01	s02	s03
s11	s12	s13	s10
s22	s23	s20	s21
s33	s30	s31	s32

After ShiftRows

s'00	s'01	s'02	s'03
s'11	s'12	s'13	s'10
s'22	s'23	s'20	s'21
s'33	s'30	s'31	s'32

After MixColumns

Round 2

s'00	s'01	s'02	s'03
s'12	s'13	s'10	s'11
s'20	s'21	s'22	s'23
s'32	s'33	s'30	s'31

s''00	S''01	s''02	s''03
s''12	s''13	s''10	s''11
s''20	s''21	s''22	s''23
s''32	s''33	s''30	s''31

Note: AddRoundKey has no impact on diffusion

Avalanche effect

- Key: 0f1571c947d9e8590cb7add6af7f6798
- Plaintext:

  0123456789abcdeffedcba9876543210

  0023456789abcdeffedcba9876543210
- Ciphertext

  ffob844a0853bf7c6934ab4364148fb9

  612b89398d0600cde11627ce72433f0

  58-Bit
- Plaintext:

  0123456789abcdeffedcba9876543210
- Key:

  0f1571c947d9e8590cb7add6af7f6798

  0e1571c947d9e8590cb7add6af7f6798
- Ciphertext:

  ffob844a0853bf7c6934ab4364148fb9

  fc8923ee501a7d207ab670686839996b

  53-Bit

Important characteristics of AES

- Security
- Brute-Force Attack
  - AES is definitely more secure than DES due to the larger-size key.
- Differential and Linear Attacks
- There are no differential and linear attacks on AES as yet.

Strength against known attacks

- Differential cryptanalysis(DC)
  - First described by Eli Biham and Adi Shamir in 1991.
  - A differential propagation is composed of differential trails(DT), where its prop ratio(PR) is the sum of the PRs of all DTs that have the specified initial and final difference patterns.
  - Necessary condition to be resistant against DC: No DT with predicated PR > 2^{-n+1}, n the block length.
  - For Rijndael: No 4-round DT with predicated PR above 2^{-150} (no 8-round trails with PR above 2^{-300}).

Strength against known attacks

- Linear cryptanalysis(*LC*)
  - First described by M. Matsui in 1994.
  - An input-output correlation is composed of linear trails (LT) that have the specified initial and final selection patterns.
  - Necessary condition to be resistant against *LC*: No LTs with a correlation coefficients > $2^{n/2}$
  - For Rijndael: No 4-round LTs with a correlation above 2^{-75} (no 8-round trails with a correlation above 2^{-150}).

Implementation

- Implementation
  - AES can be implemented in software, hardware, and firmware. The implementation can use table lookup process or routines that use a well-defined algebraic structure
  - Each Encryption round Function
    - Can be collapsed to 4 table lookups and 4 XORs using 32-bit values (tables for last round differ – no MixColumns step)
    - XOR result with round key
- Simplicity
  - The algorithms used in AES are so simple that they can be easily implemented using cheap processors and a minimum amount of me*mory*.

- AES Block Ciphers

Another Mode of Encryption

XTS-AES Mode

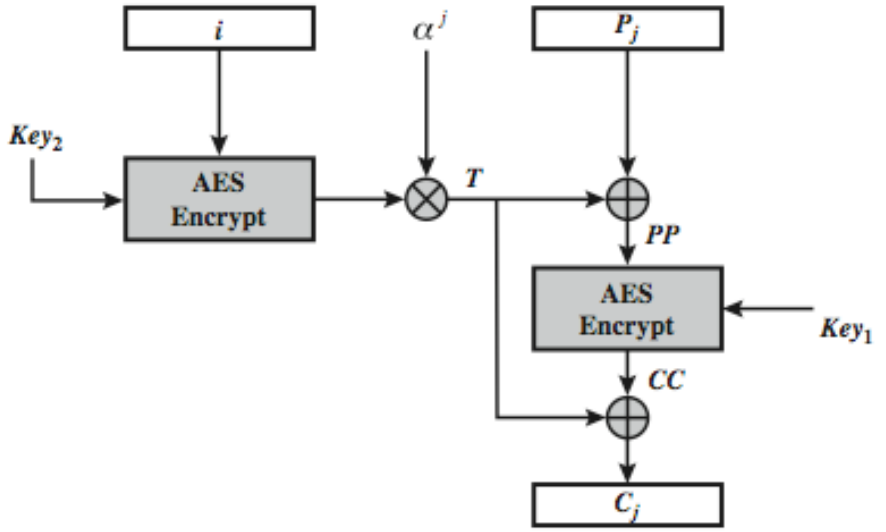
- A mode, for block oriented storage use
  - in IEEE Std 1619-2007
  - different requirements to transmitted data
- concept of tweakable block cipher
  - uses AES twice for each block

$$T_j = E_{K2}(i) \text{ XOR } \alpha^j$$

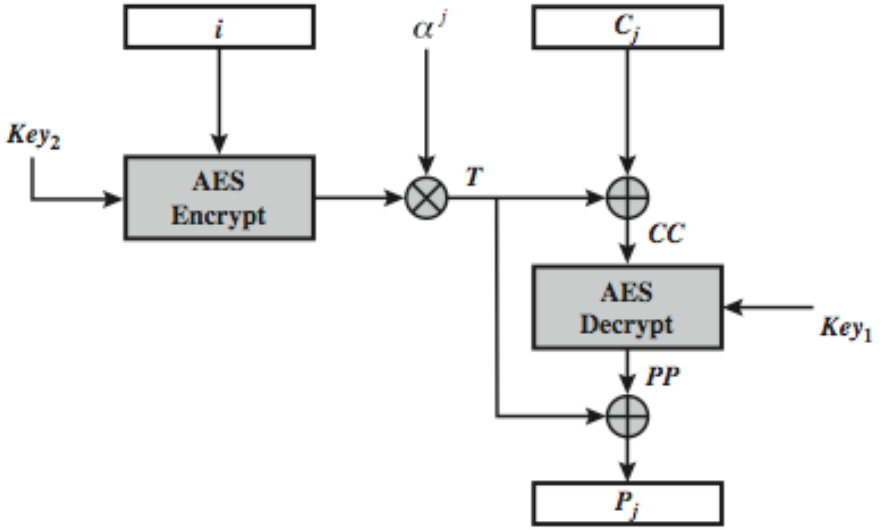
$$C_j = E_{K1}(P_j \text{ XOR } T_j) \text{ XOR } T_j$$

  where i is tweak for the sector & j is block no
  - each sector may have multiple blocks

XTS-AES Mode per block

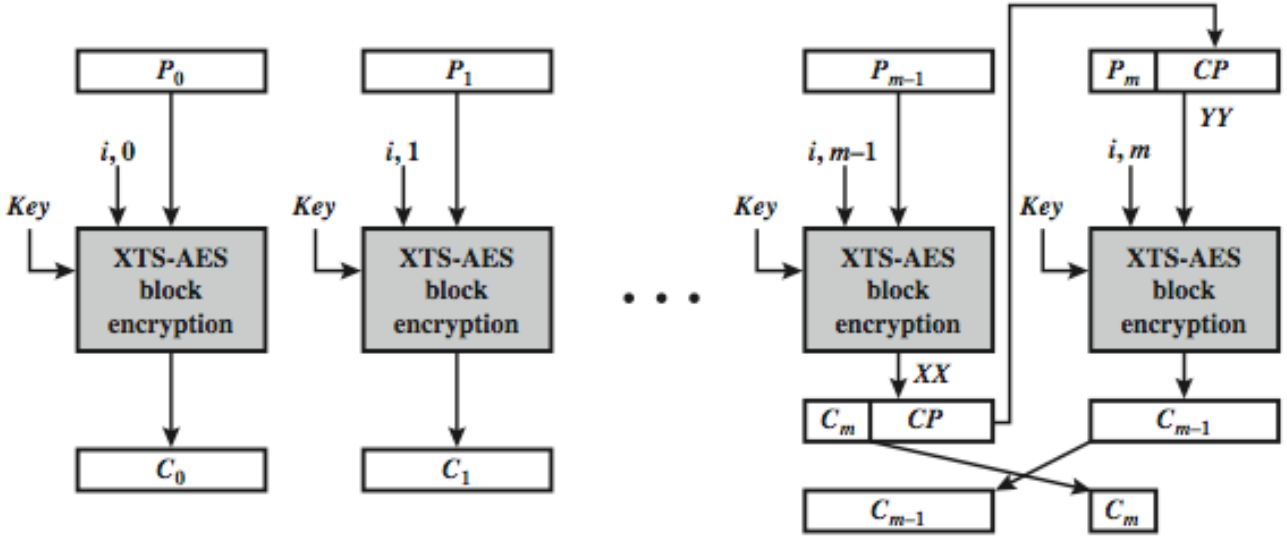


(a) Encryption

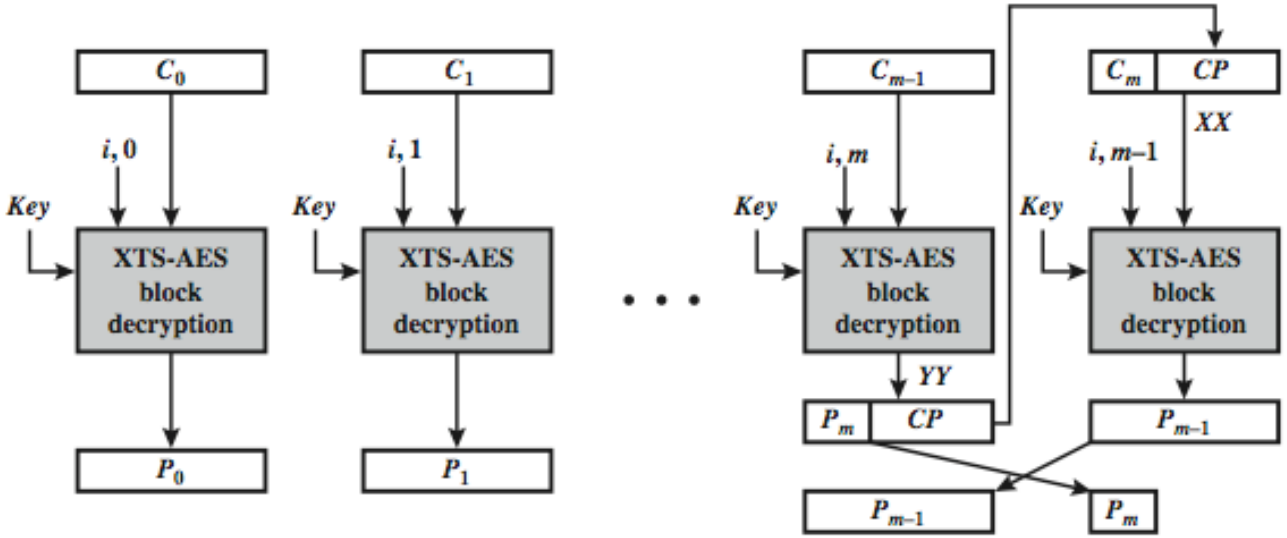


(b) Decryption

XTS-AES Mode Overview



(a) Encryption



(b) Decryption

- Thanks