CS557: Cryptography

Modern Ciphers (AES)

S. Tripathy
IIT Patna

We discussed

- Modern Cipher
  - Block cipher
    - DES
    - Cryptanalysis
      - Linear Cryptanalysis
      - Differential Cryptanalysis
    - 3DES
    - AES

AES: Advance Encryption Standard

- clear a replacement for DES was needed
  - have theoretical attacks that can break it
  - have demonstrated exhaustive key search attacks
- can use Triple-DES – but slow with small blocks

- NIST announced Call for ciphers in 1997
  - 15 candidates accepted in Jun 98
  - 5 were short-listed in Aug-99
  - Rijndael was selected as the AES in Oct-2000
  - issued as FIPS PUB 197 standard in Nov-2001

Requirements - NIST

- Security:
  - Resistance to cryptanalysis
  - Soundness of the mathematical basis
  - Randomness of the ciphertext

- Costs:
  - System resources (hardware and software) required
  - Monetary costs

- Algorithm and implementation characteristics
  - Simplicity: reduces implementation errors and impacts costs, such as power consumption, number of hardware gates and execution time
  - Encryption and decryption using the same algorithm
  - Ability to implement the algorithm in both software and hardware
  - Use for other cryptographic purposes (hash function, a random bit generator and a stream cipher - such as via CTR mode)

AES Competetion

	Rijndael	Serpent	Twofish	MARS	RC6
General Security	2	3	3	3	2
Implementation Difficulty	3	3	2	1	1
Software Performance	3	1	1	2	2
Smart Card Performance	3	3	2	1	1
Hardware Performance	3	3	2	1	2
Design Feature	2	1	3	2	1
Total	16	14	13	10	9

I Won

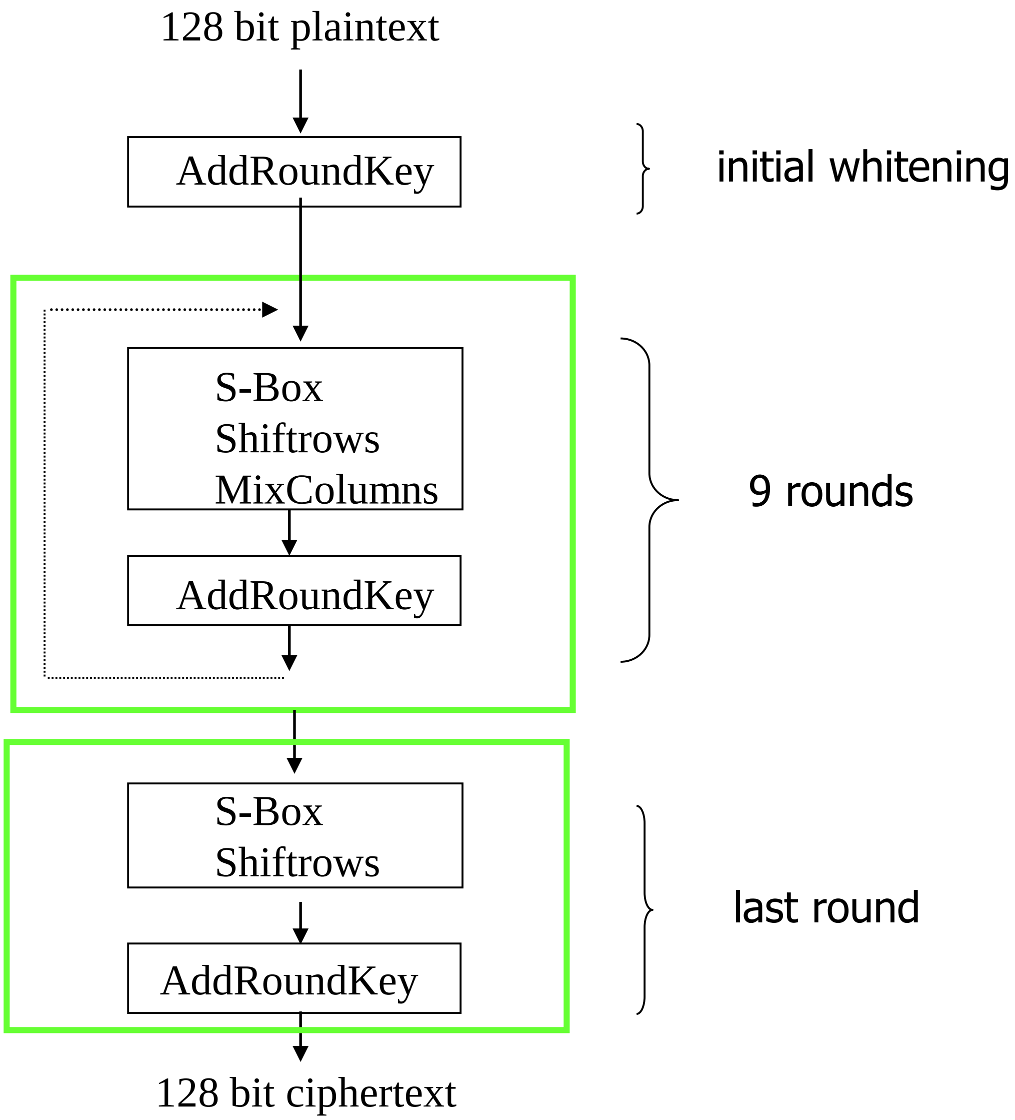
AES

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

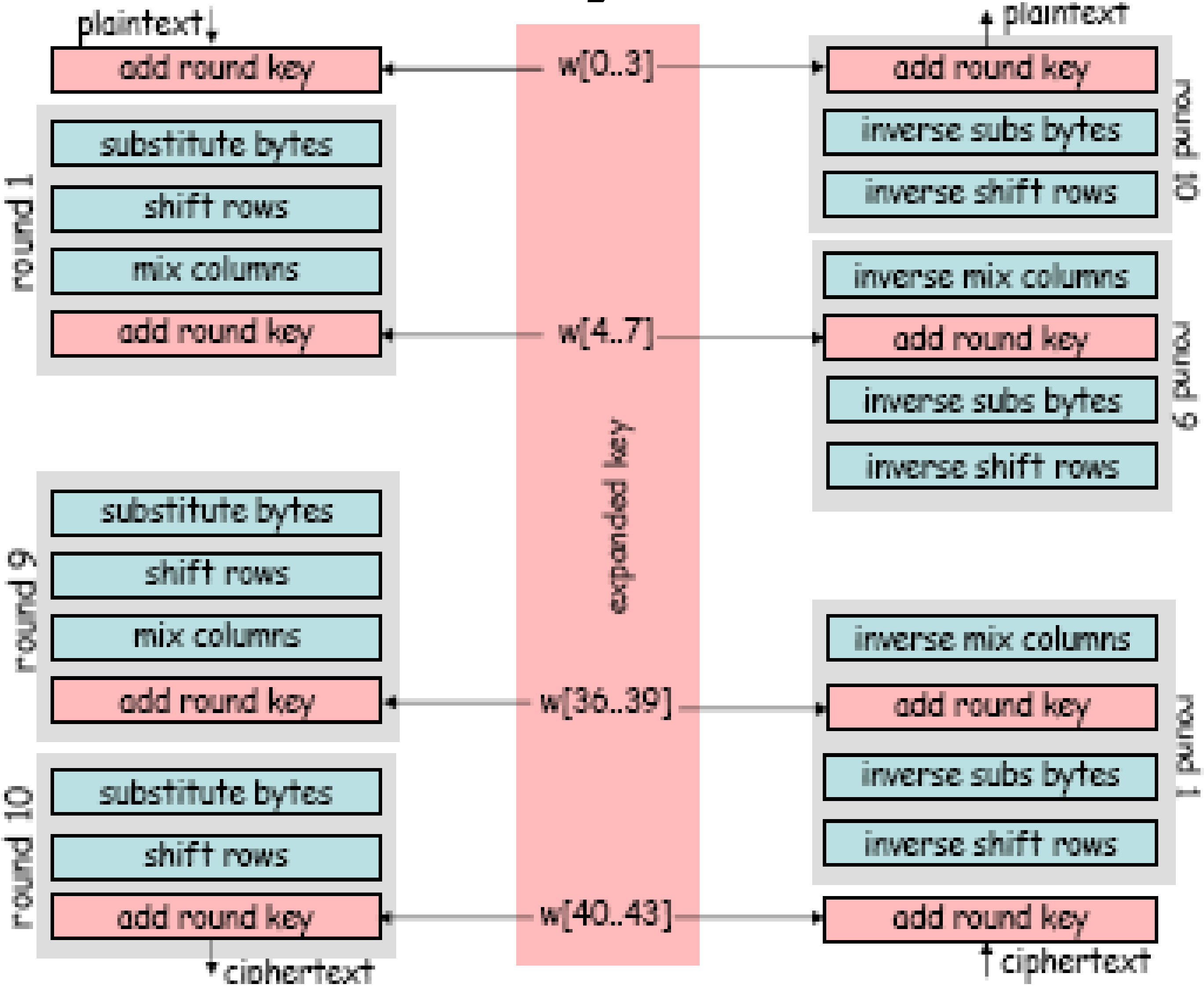
- **Decryption algorithm is different from encryption algorithm (non Feistel structure). (optimized for encryption)**

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

AES – 128 bit block



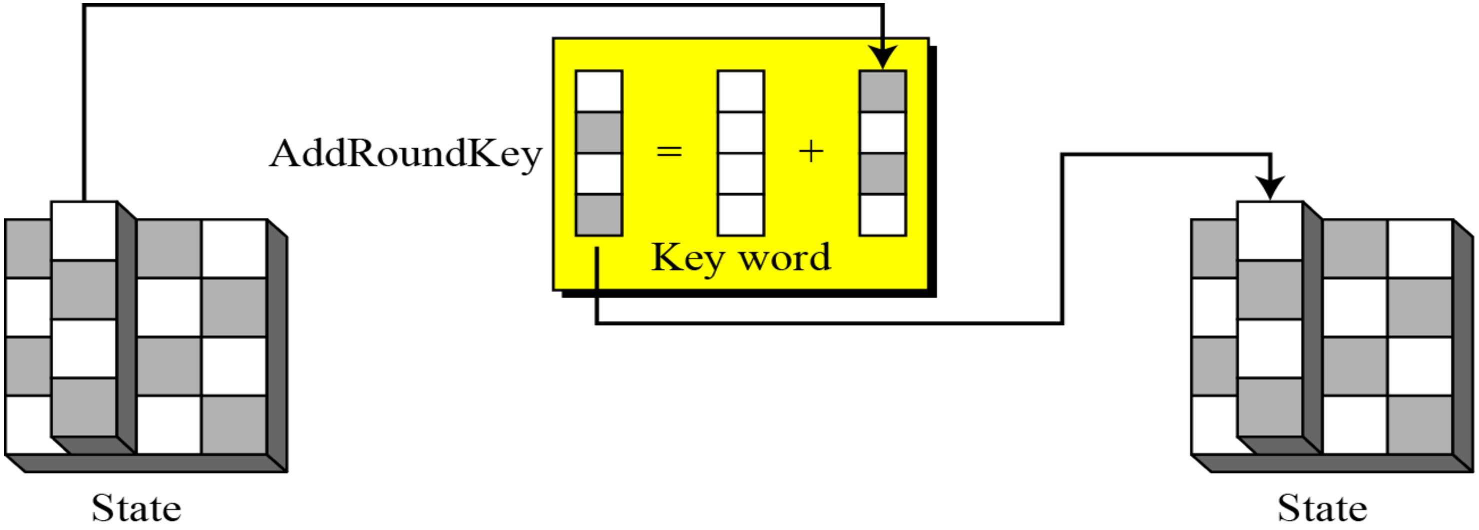
AES-Rijndael



AES Round Function Components:

Add Round Key

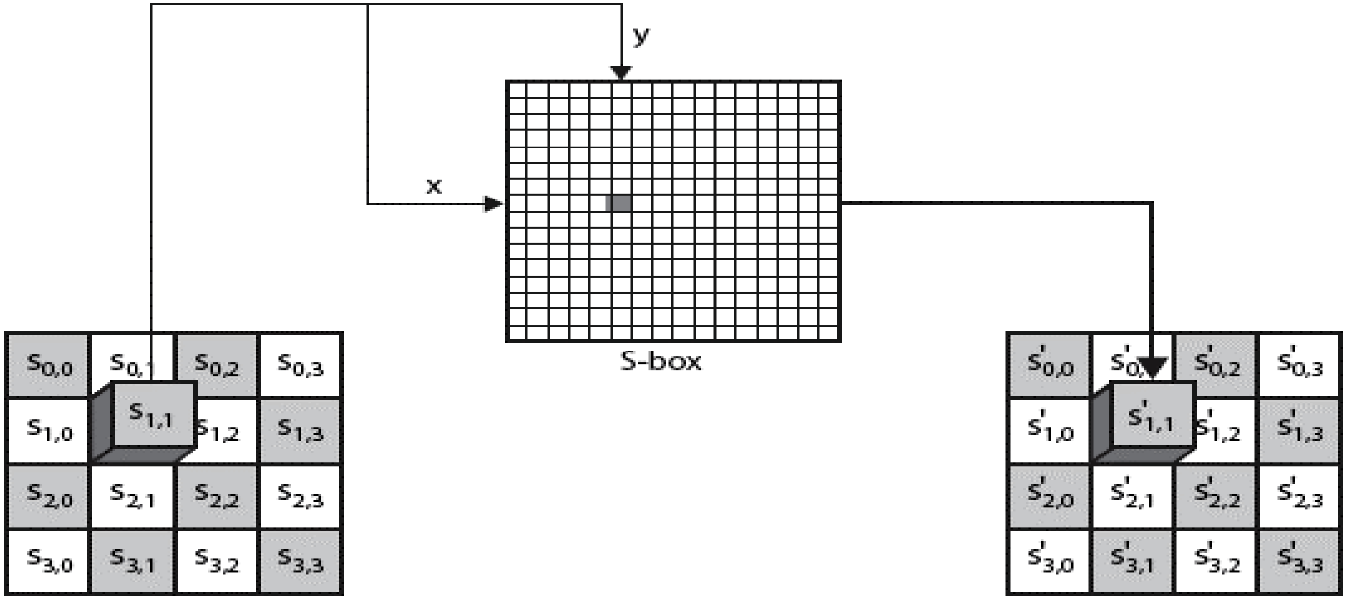
- AddRoundKey proceeds one column at a time.
- AddRoundKey adds a round key word with each state column matrix; the operation in AddRoundKey is matrix addition



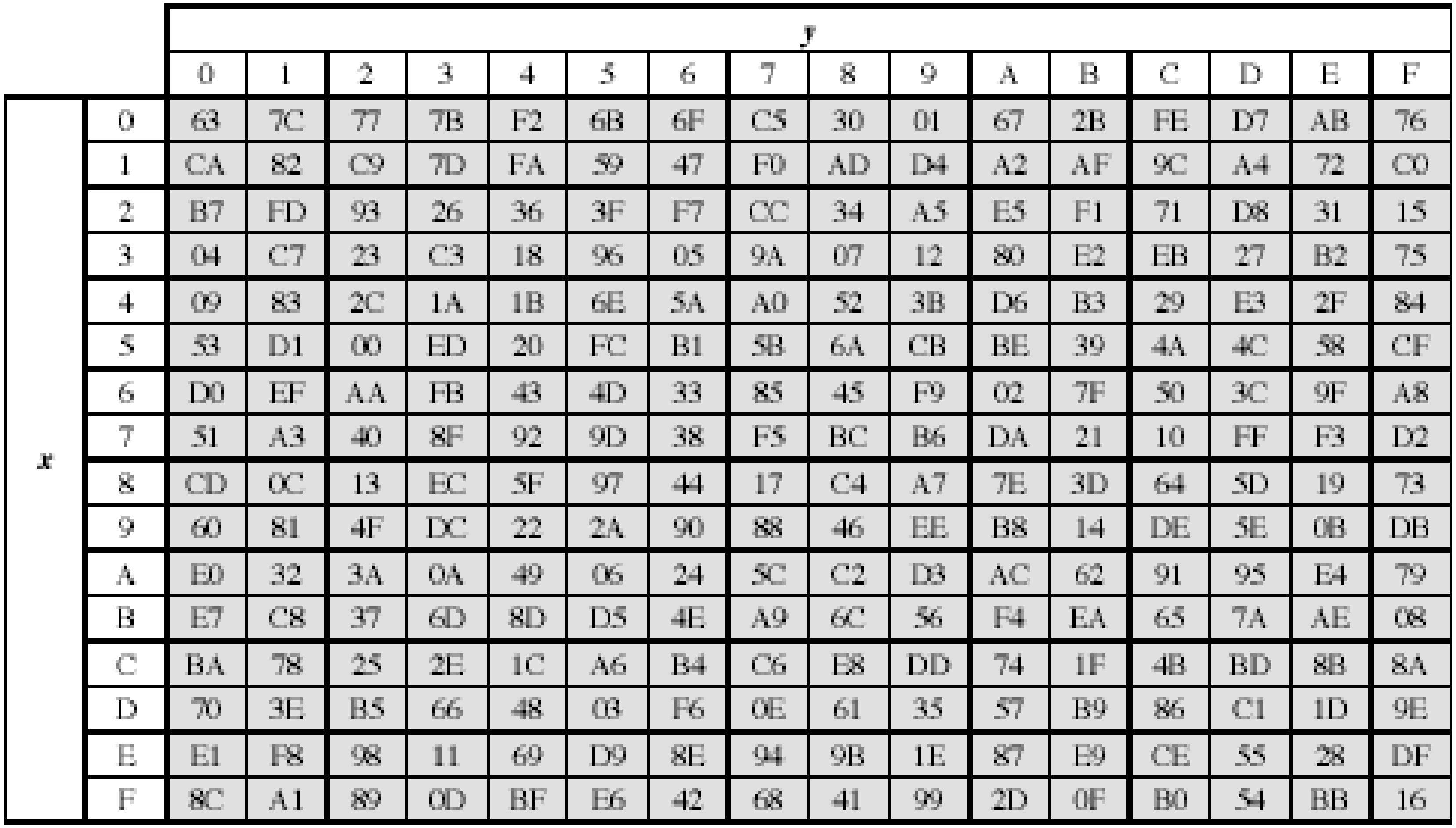
AES Round Function Components:

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 $y = Ax^{-1} + c$

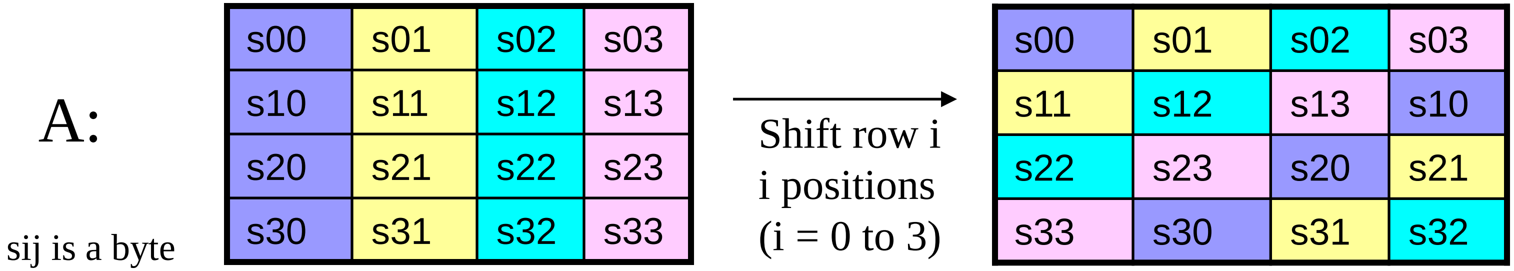
$$\begin{bmatrix} s_0 \\ s_1 \\ s_2 \\ s_3 \\ s_4 \\ s_5 \\ s_6 \\ s_7 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\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

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

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

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)

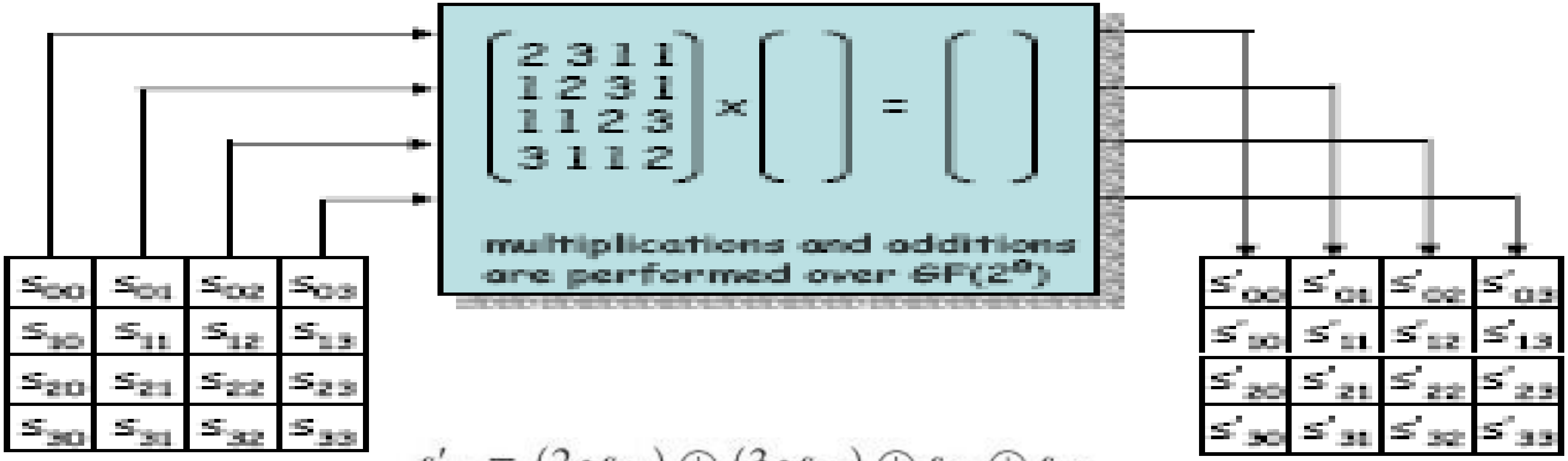
s00	s01	s02	s03
s11	s12	s13	s10
s22	s23	s20	s21
s33	s30	s31	s32

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*



$$\begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix} \times \begin{bmatrix} \; \end{bmatrix} = \begin{bmatrix} \; \end{bmatrix}$$

multiplications and additions are performed over GF(2^8)

s_{00}	s_{01}	s_{02}	s_{03}
s_{10}	s_{11}	s_{12}	s_{13}
s_{20}	s_{21}	s_{22}	s_{23}
s_{30}	s_{31}	s_{32}	s_{33}

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

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

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.

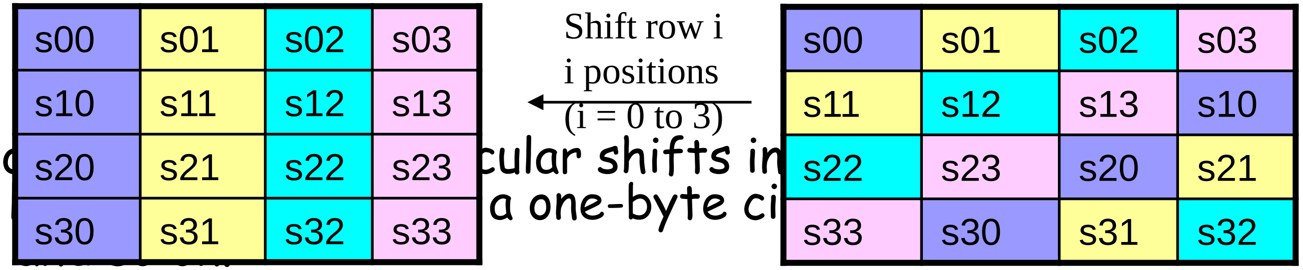
$$A \leftarrow \text{round\_key} \oplus A$$

❑ **Inverse SubBytes:**

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

❑ **InvShiftRows:**

- Inverse Shift R … 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:**

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

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