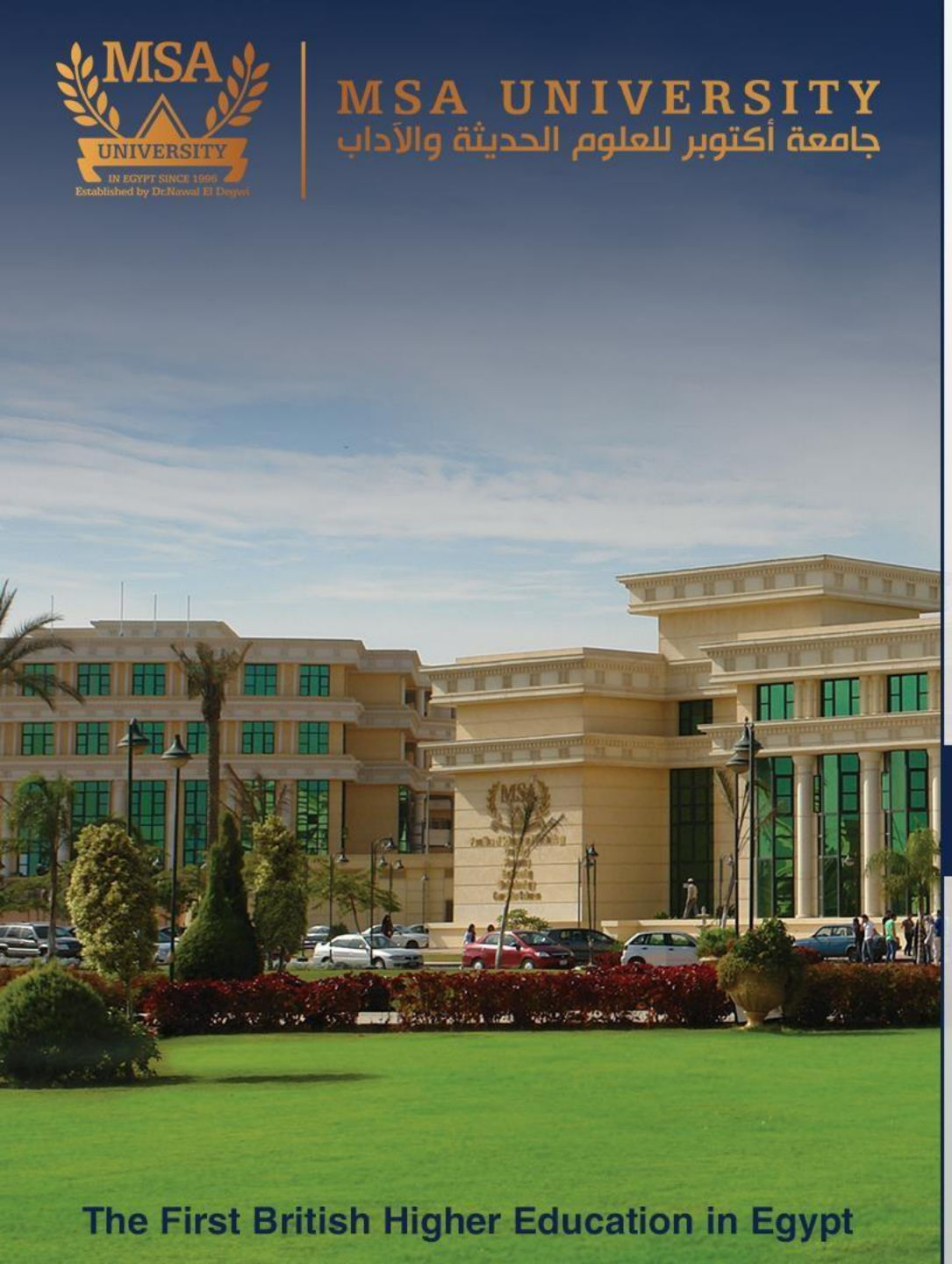
MSA UNIVERSITY
جامعة أكتوبر للعلوم الحديثة والآداب



Cryptography
ECE5632 - Spring 2024

Lecture 6B

Dr. Farah Raad

Lecture Topic

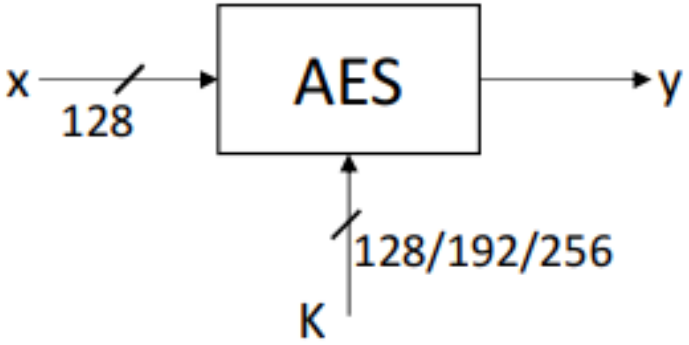
The Advanced Encryption Standard (AES)

The Advanced Encryption Standard (AES)

- AES is the most widely used symmetric cipher today.
- Found in every web browser, in banking machines, WiFi routers, etc ..

❖ The requirements for all AES candidate submissions were:

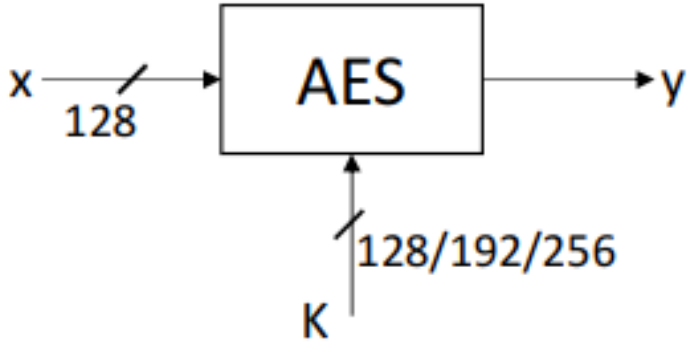
- Block cipher with **128-bit block size**
- **Three supported key lengths**: 128, 192 and 256 bit
- Security relative to other submitted algorithms
- **Efficiency** in software and hardware



The Advanced Encryption Standard (AES)

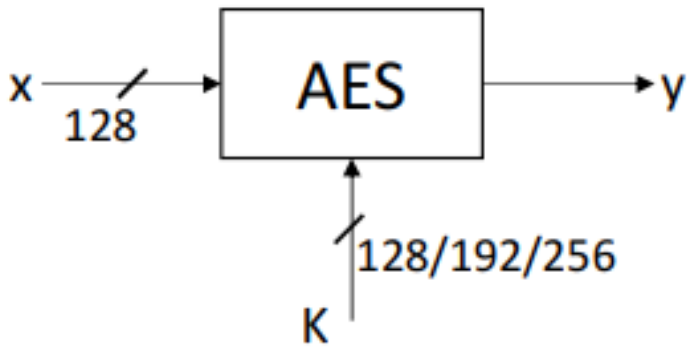
- **The number of rounds depends on the chosen key length:**

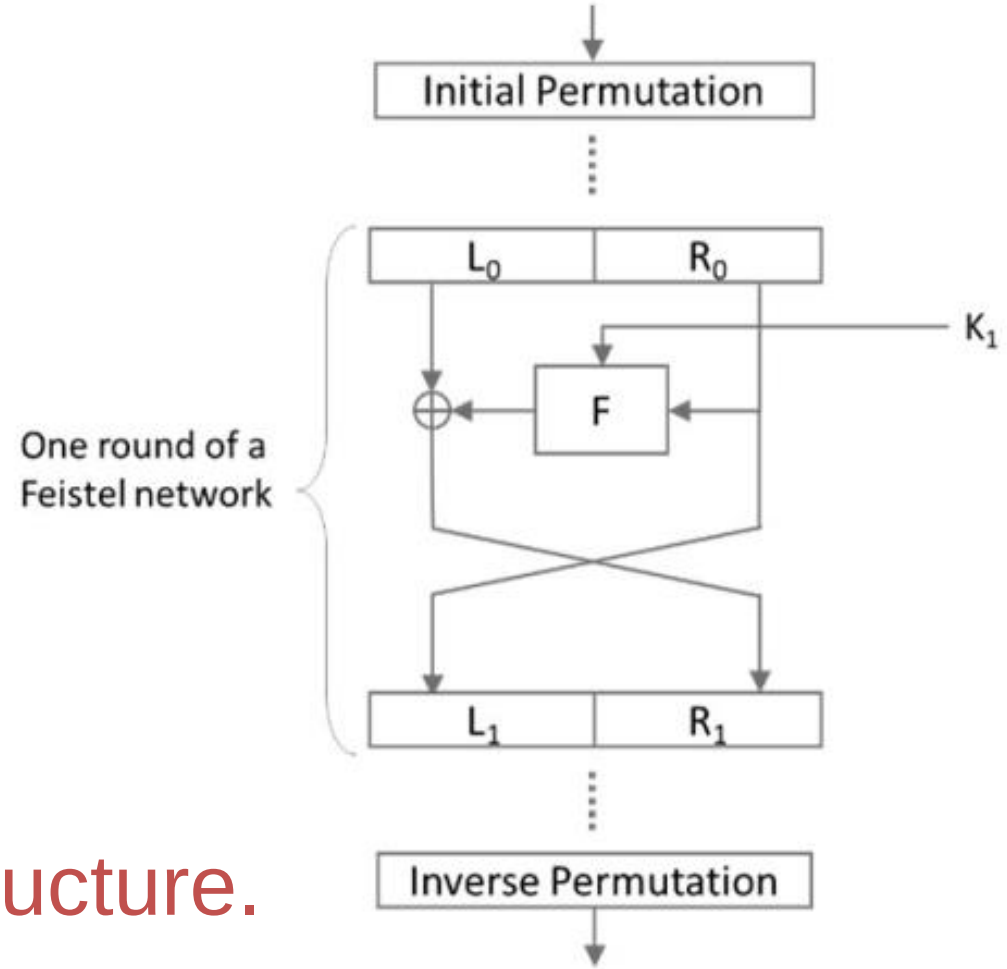
Key length (bits)	Number of rounds
128	10
192	12
256	14



Structure of AES

✓ Remember the Feistel structure? (e.g., SDES, DES)



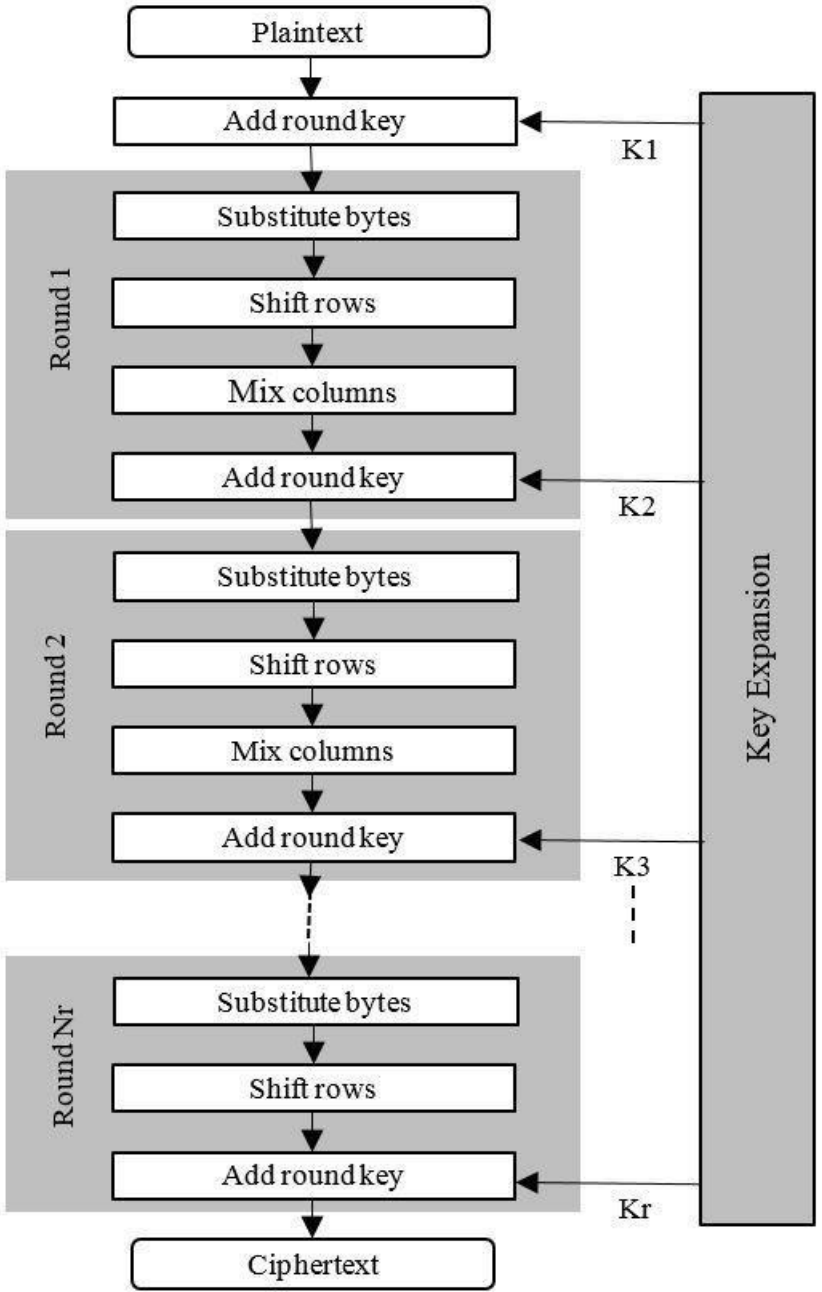


AES does **NOT** use the Feistel structure.

Structure of AES

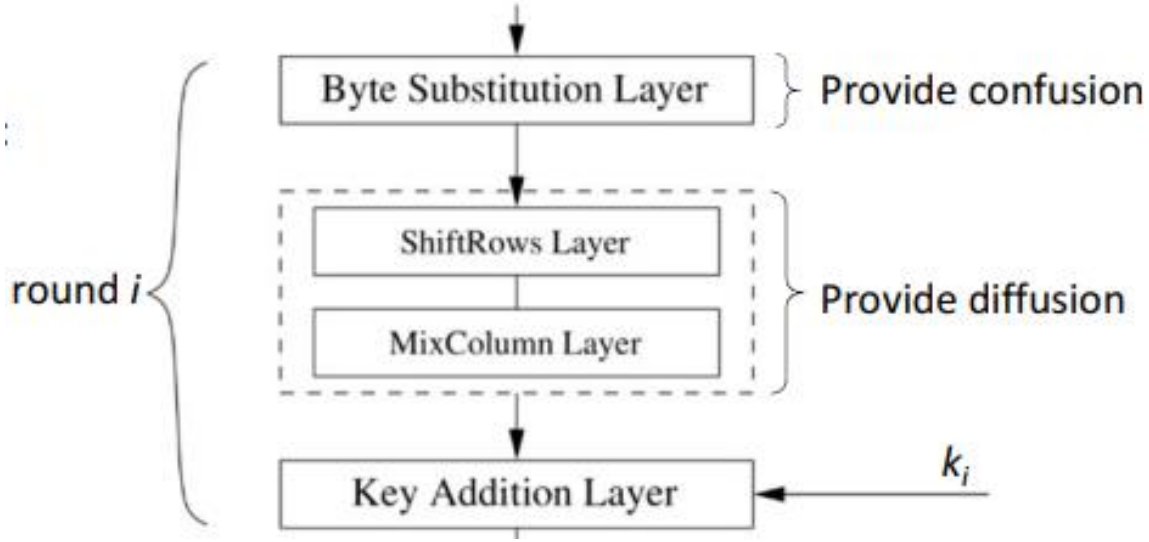
- AES encrypts all 128 bits of the data path in each round.
- A subkey is added at the beginning and at the end of encryption (**key whitening**)
- AES number of rounds depend on the key length:

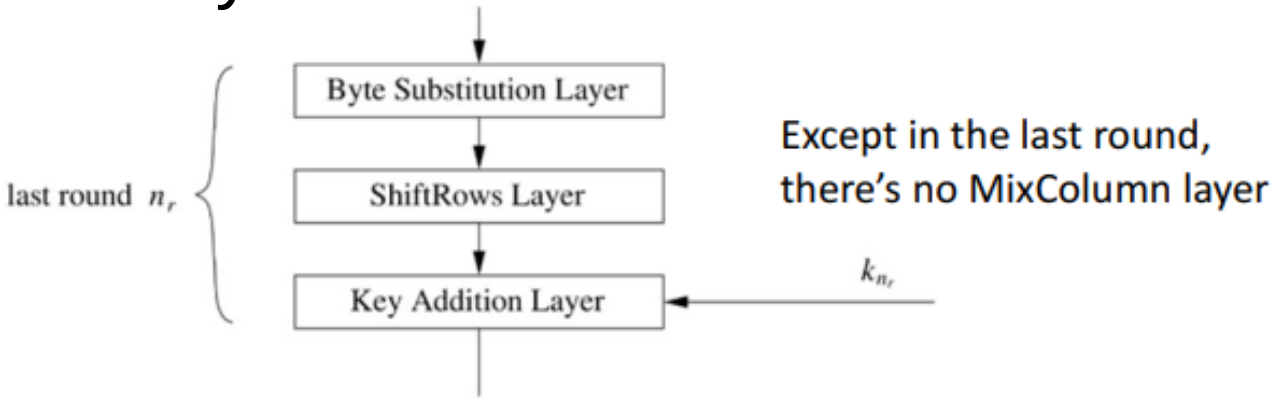
key length	# rounds = n_r
128 bit	10
192 bit	12
256 bit	14



Structure of AES

- Each round consists of 4 layers:
  1) Byte Subsitution
  2) Shift Row
  3) Mix Column
  4) Key Addition
- Except in the last round, there's no Mix Column layer





Structure of AES

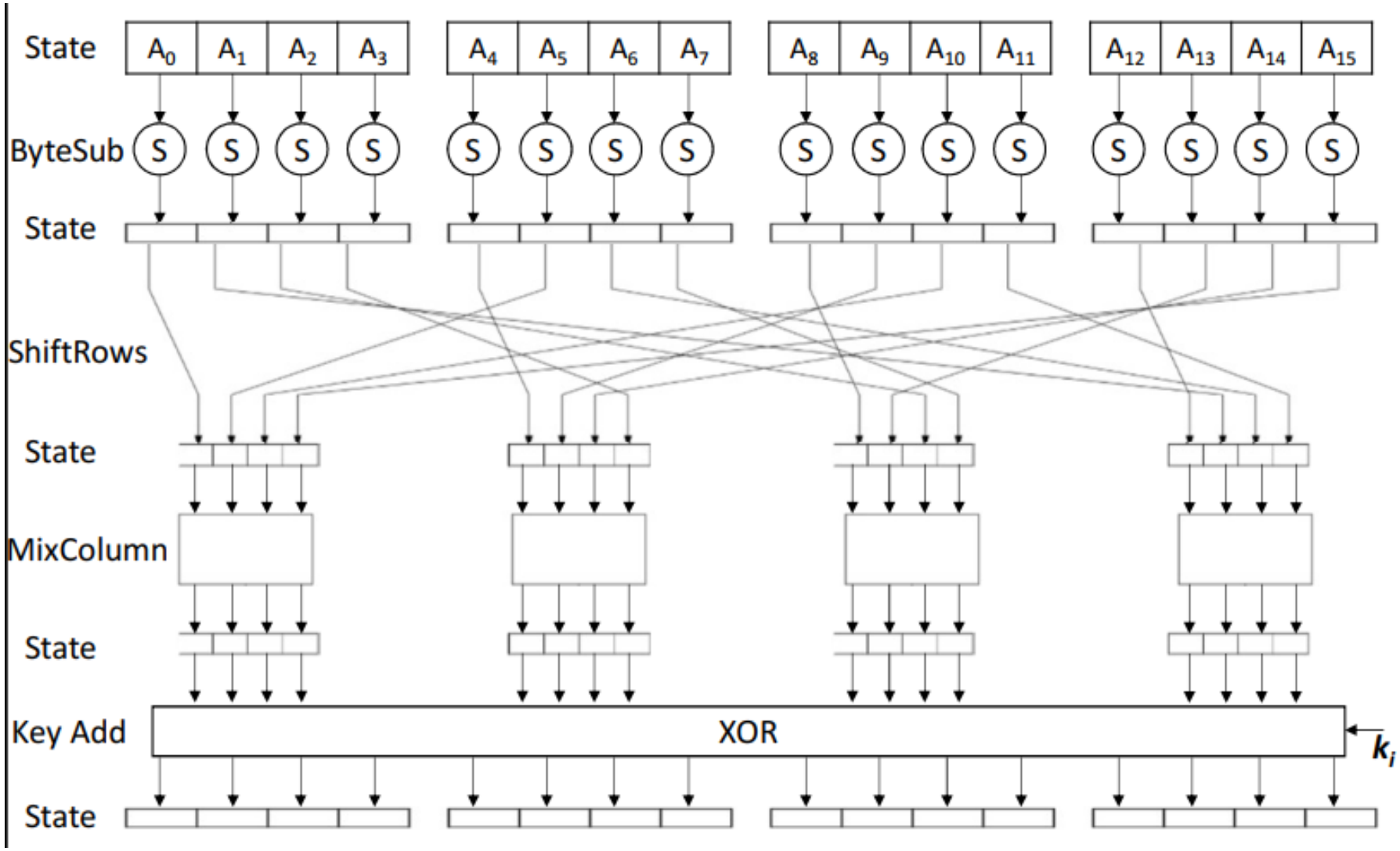
- **Note:** AES is byte oriented cipher.
- The 128 bit data block (data path) is split into 16 bytes.
- with A0,…, A15 denoting the 16-byte input of AES

A_0	A_1	A_2	A_3	A_4	A_5	A_6	A_7	A_8	A_9	A_{10}	A_{11}	A_{12}	A_{13}	A_{14}	A_{15}

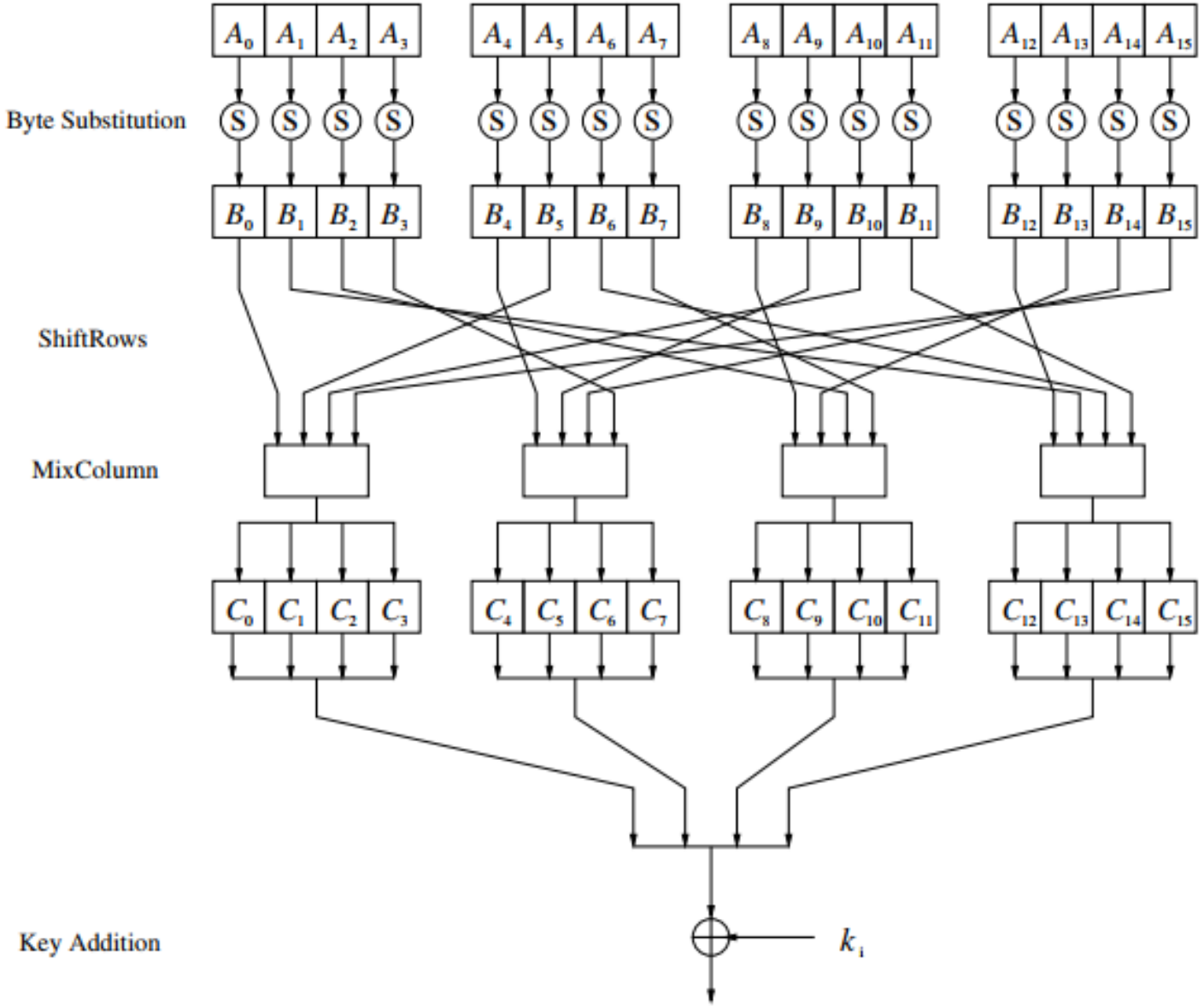
Bytes A_0 , A_1 , . . . , A_{15} are arranged in a four-by-four byte matrix called the <u>state</u>.

A_0	A_4	A_8	A_{12}
A_1	A_5	A_9	A_{13}
A_2	A_6	A_{10}	A_{14}
A_3	A_7	A_{11}	A_{15}

AES Encryption Round



AES Encryption Round



AES Internals

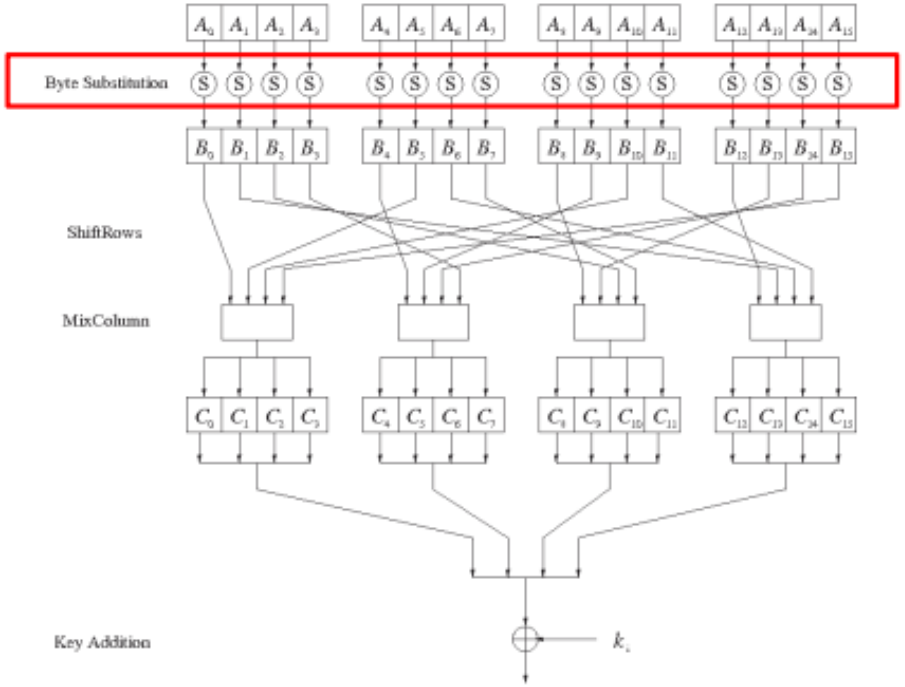
a) The Byte Substitution Layer:

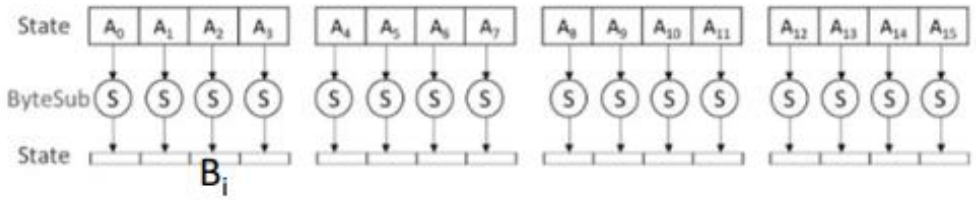
- The Byte Substitution layer consists of 16 **S-Boxes** with the following properties:

  The S-Boxes are

  - **identical**
  - the only **nonlinear** elements of AES, i.e., $\text{ByteSub}(A_i) + \text{ByteSub}(A_j) \neq \text{ByteSub}(A_i + A_j)$, for $i,j = 0,\ldots,15$
  - **bijective**, i.e., there exists a one-to-one mapping of input and output bytes

    $\Rightarrow$ S-Box can be uniquely reversed

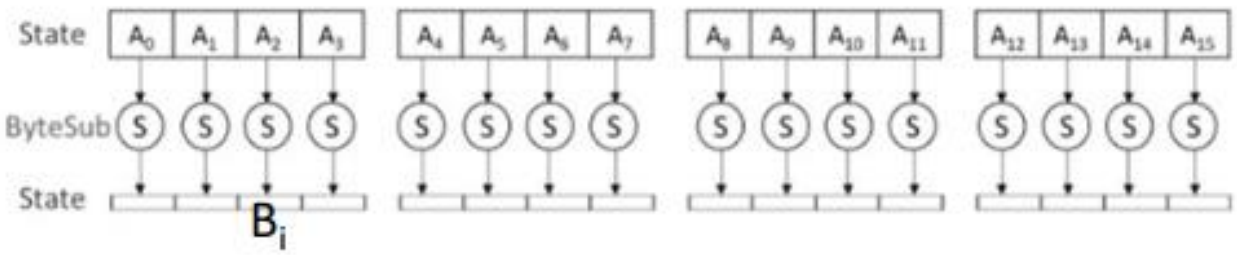




- In software implementations, the S-Box is usually realized as a lookup table

AES Internals

a) The Byte Substitution Layer:

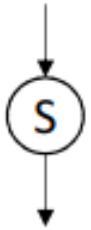


Example

$A_i = C2_{16} = (xy)$

$B_i = S(A_i) = 25_{16}$

1100 0010



0010 0101

AES S-Box: Substitution values in hexadecimal notation for input byte (xy)

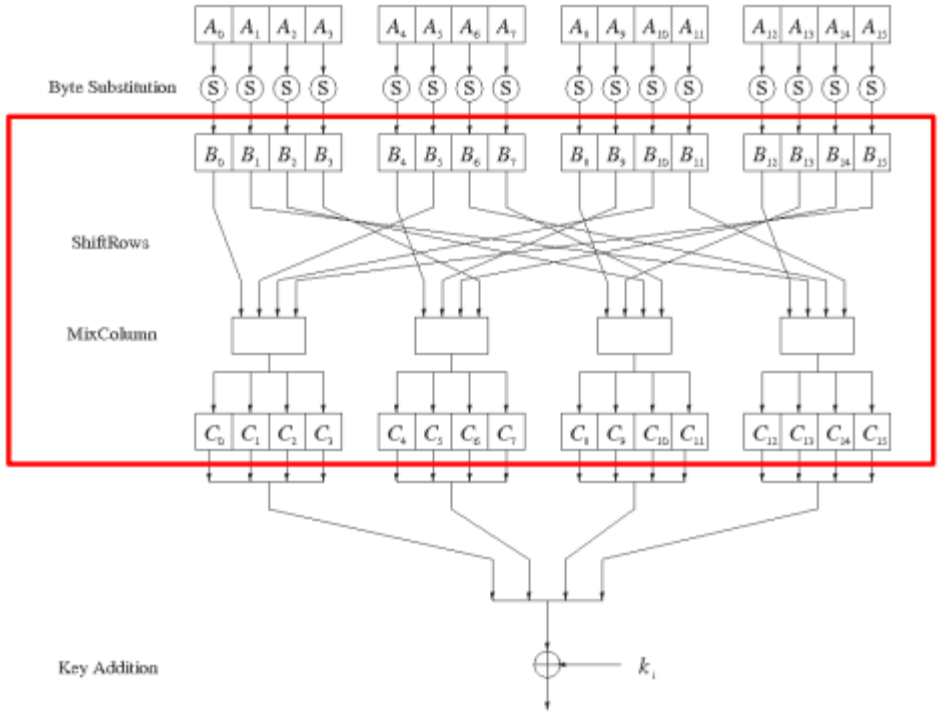
x \ y	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
5	53	D1	00	ED	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 Internals (Diffusion Layer)

b) The Diffusion layerr:

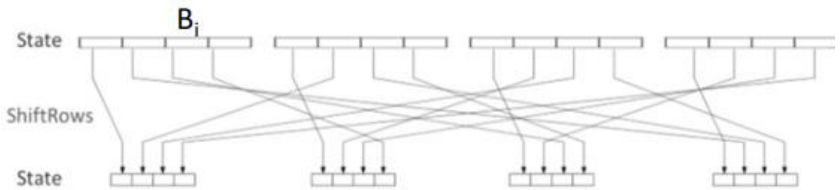
- provides diffusion over all input state bits
- consists of two sublayers:
  - **ShiftRows Sublayer**: Permutation of the data on a byte level
  - **MixColumn Sublayer**: Matrix operation which combines ("mixes") blocks of four bytes
- performs a linear operation on state matrices A, B, i.e.,

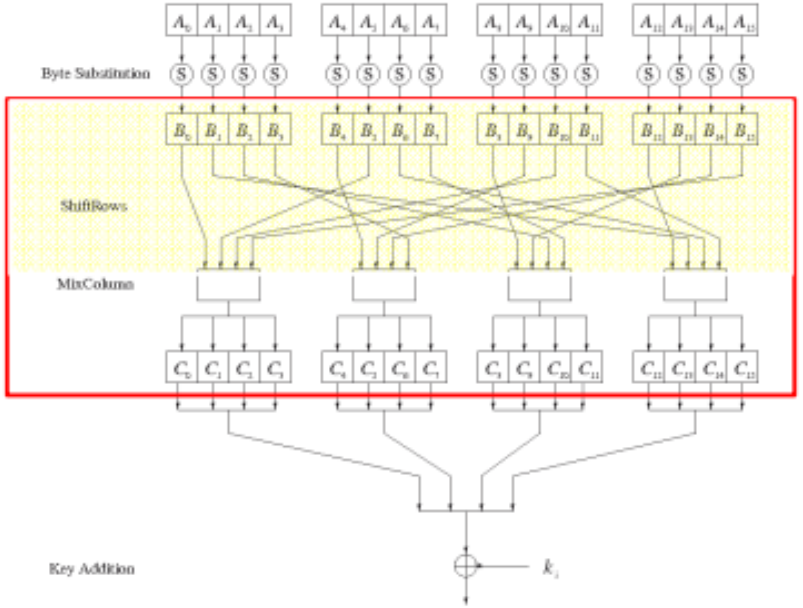
$$\mathrm{DIFF}(A) + \mathrm{DIFF}(B) = \mathrm{DIFF}(A + B)$$



AES Internals (Diffusion Layer)

1) Shift Rows Sublayer:





Outputs of 16 S-Boxes are rolled in a 4x4 state matrix:

B_0	B_4	B_8	B_{12}
B_1	B_5	B_9	B_{13}
B_2	B_6	B_{10}	B_{14}
B_3	B_7	B_{11}	B_{15}

After the Shift Rows operation, the new state matrix becomes as follows:

B_0	B_4	B_8	B_{12}	no shift
B_5	B_9	B_{13}	B_1	⟵ one position left shift
B_{10}	B_{14}	B_2	B_6	⟵ two positions left shift
B_{15}	B_3	B_7	B_{11}	⟵ three positions left shift

So, the input to the next layer becomes:

B_0	B_5	B_{10}	B_{15}	B_4	B_9	B_{14}	B_3	B_8	B_{13}	B_2	B_7	B_{12}	B_1	B_6	B_{11}

Input matrix

B_0	B_4	B_8	B_{12}
B_1	B_5	B_9	B_{13}
B_2	B_6	B_{10}	B_{14}
B_3	B_7	B_{11}	B_{15}

Output matrix

B_0	B_4	B_8	B_{12}
B_5	B_9	B_{13}	B_1
B_{10}	B_{14}	B_2	B_6
B_{15}	B_3	B_7	B_{11}

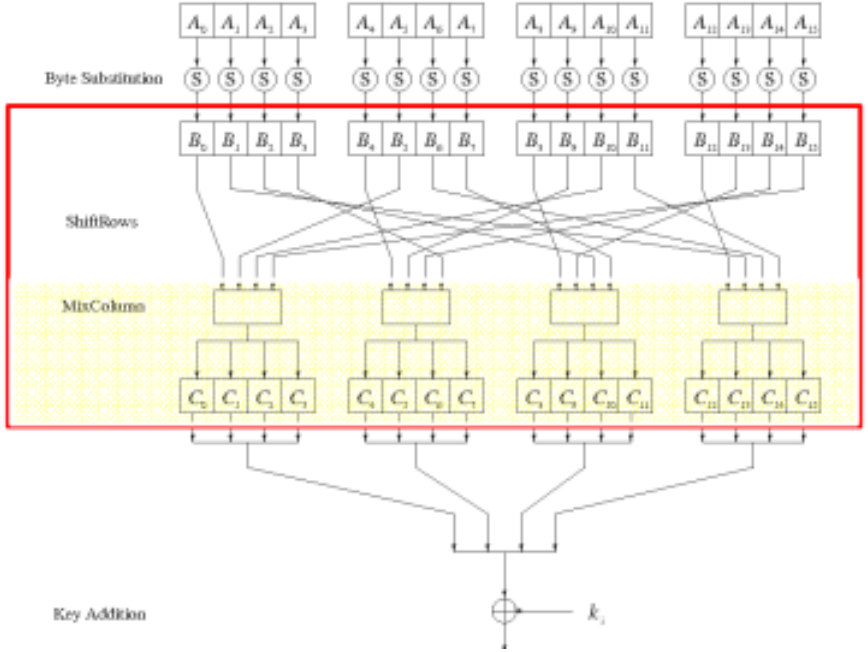
AES Internals (Diffusion Layer)

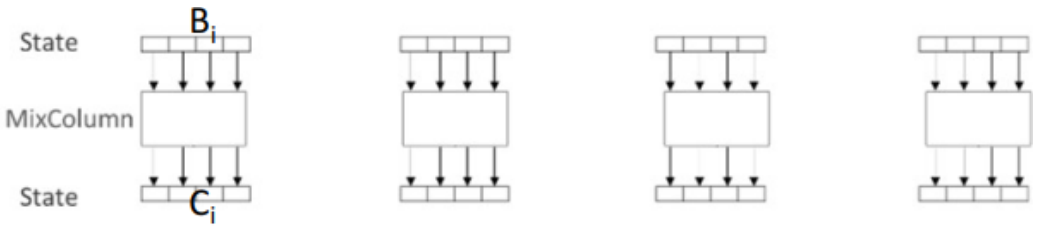
2. MixColumn Sublayer

- Each 4-byte column is considered as a vector and multiplied by a fixed 4x4 matrix, e.g.,

$$\begin{pmatrix} C_0 \\ C_1 \\ C_2 \\ C_3 \end{pmatrix} = \begin{pmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{pmatrix} \cdot \begin{pmatrix} B_0 \\ B_5 \\ B_{10} \\ B_{15} \end{pmatrix}$$

where 01, 02 and 03 are given in hexadecimal notation



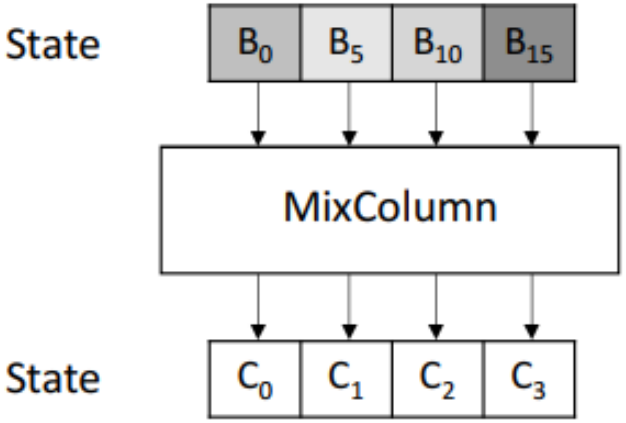


AES Internals (Diffusion Layer)

2. MixColumn Sublayer

Example:

1st MixColumn Box (other three are identical)



$$\begin{pmatrix} C_0 \\ C_1 \\ C_2 \\ C_3 \end{pmatrix} = \begin{pmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{pmatrix} \begin{pmatrix} B_0 \\ B_5 \\ B_{10} \\ B_{15} \end{pmatrix}$$

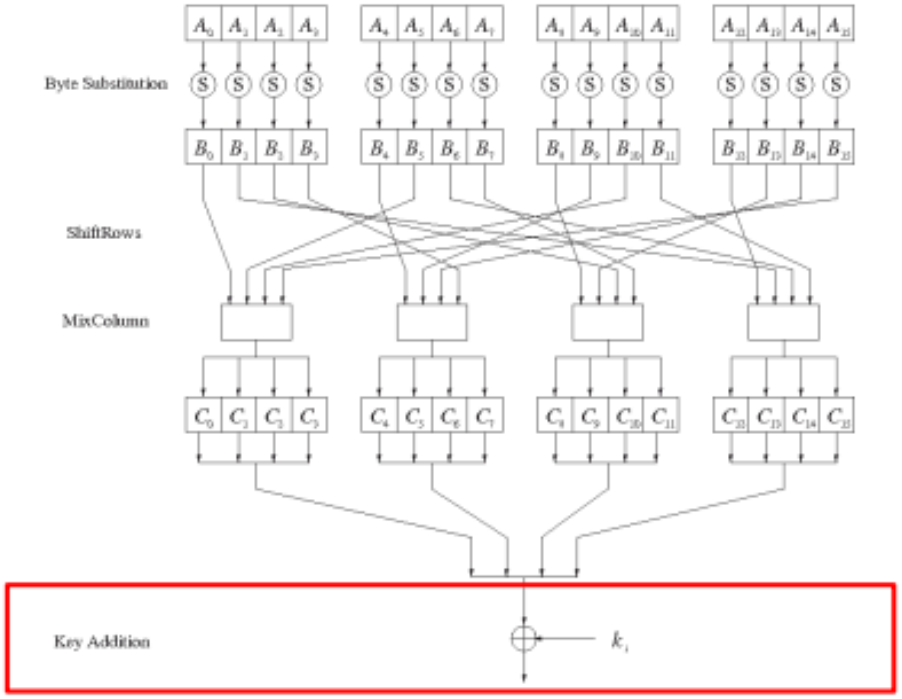
This way, 1 bit flip in any of the input bytes affects C_0, C_1, C_2, C_3.

Note: The multiplications and additions for each C_i is done in $GF(2^8)$ with $P(x) = x^8 + x^4 + x^3 + x + 1$

AES Internals

c. Key Addition Layer

- Inputs:
  - 16-byte state matrix C
  - 16-byte subkey k_i
- Output: $C \oplus k_i$
- The subkeys are generated in the key schedule



Key Schedule

- Subkeys are derived recursively from the original 128/192/256-bit input key

- Each round has 1 subkey, plus 1 subkey at the beginning of AES

Key length (bits)	Number of subkeys
128	11
192	13
256	15

- Key whitening: Subkey is used both at the input and output of AES
  $\Rightarrow$ # subkeys = # rounds + 1

- There are different key schedules for the different key sizes

MSA UNIVERSITY
IN EGYPT SINCE 1996
Established by Dr.Nawal El Degwi
MSA UNIVERSITY
جامعة أكتوبر للعلوم الحديثة والآداب

Thank You!

See You next Lectures!!
Any Question?