INF 638
Cryptography & Cryptosystems

Section 5: Advanced Encryption System

Dr. Bertrand Cambou
Professor of Practice NAU, Cybersecurity
School of Informatics, Computing, and Cyber-Systems
Bertrand.cambou@nau.edu

NORTHERN ARIZONA UNIVERSITY

INF 638: Cryptography & Cryptosystems

- 1- Motivation & Definitions
- 2- Elements of Number theory
- 3- Early Cryptographic methods
- 4- Symmetrical Cryptography: DES
- 5- Symmetrical Cryptography: AES
- 6- Quantum Cryptography: Key distribution
- 7- Elements of Asymmetrical Cryptography
- 8- Asymmetrical Cryptography: RSA
- 9- ECC Key Distribution
- 10- PKI & Digital Signatures
- 11- Hash Functions
- 12- Smartcards

5-Advanced Encryption Standard

- 5-A Finite (Galois) fields
- 5-B Advanced Encryption Standard
  - AES architecture
  - AES Key generation
  - Summary

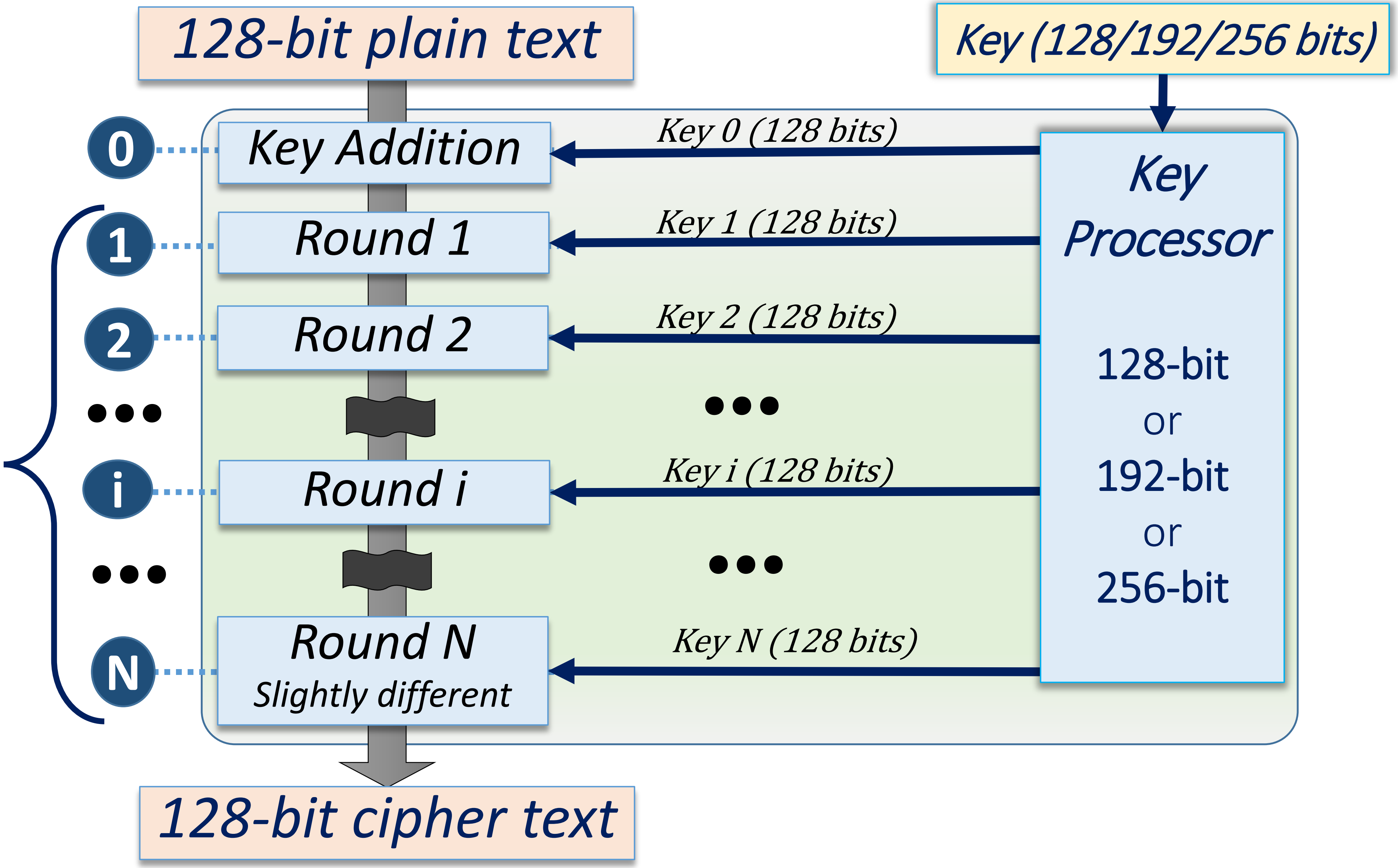
AES: Advanced Encryption Standard

- Open call for AES by NIST in **1997** – submission of 15 algorithms
- Winner: Rijndael algorithm in **2000**

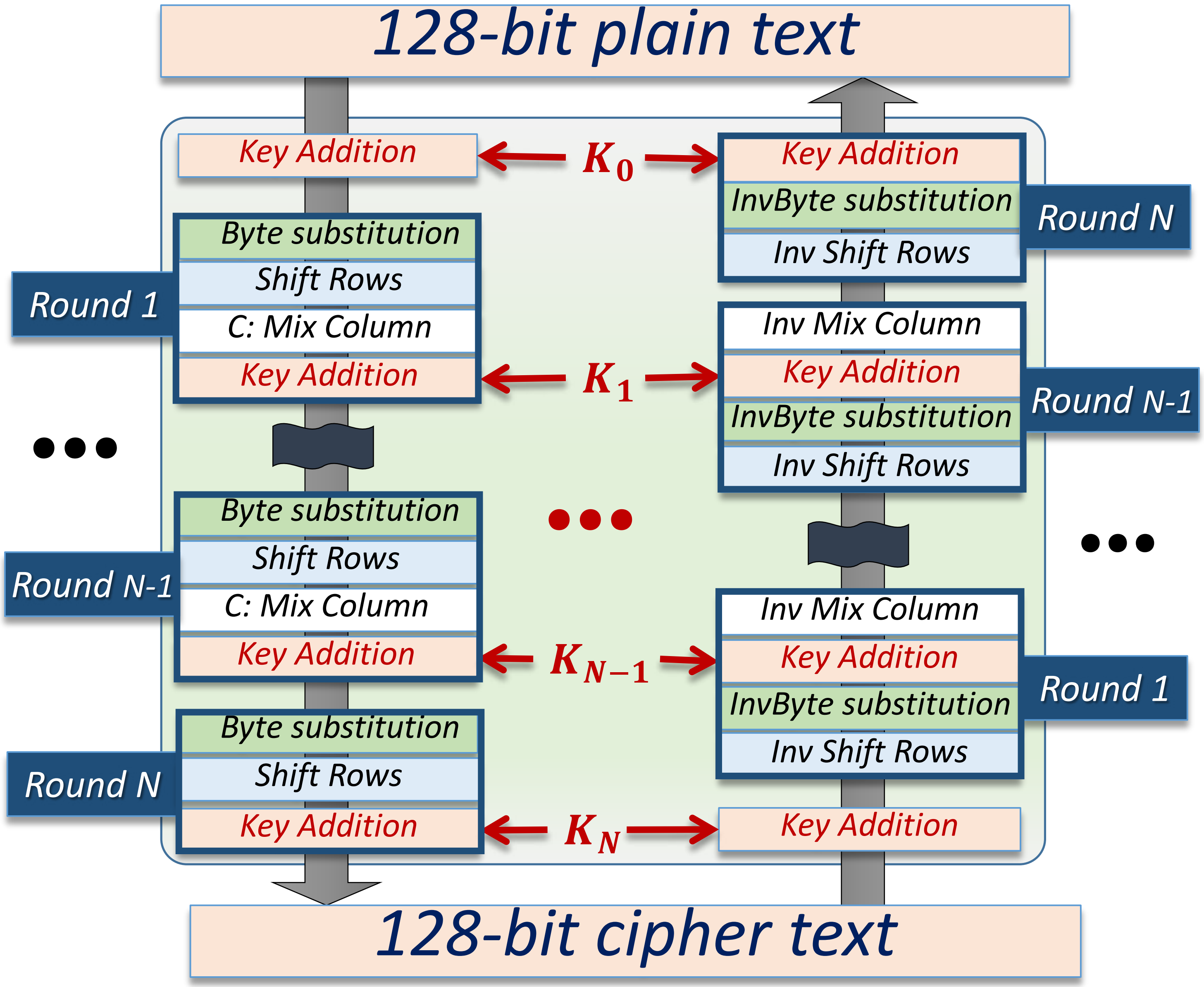
  (by Vincent Rijmen & Joan Daemen from Louvain/Belgium)
- Adopted in **2001** for commercial use, and by NSA for classified data
- AES operate on block of **128-bits** with a **128**, **192**, **256**-bit key
- Data manipulation include:
  - Diffusion, permutation, shift, mixing (use extended Galois Fields)
  - Logic functions: XOR, AND, OR
  - Repeat 10, 12, 14 times
- **AES is currently the most important symmetric algorithm with 70% acceptance**

Summary AES

Key size	Number of rounds N
128	10
192	12
256	14



AES: Encryption versus Decryption



Use extended Galois Field arithmetic

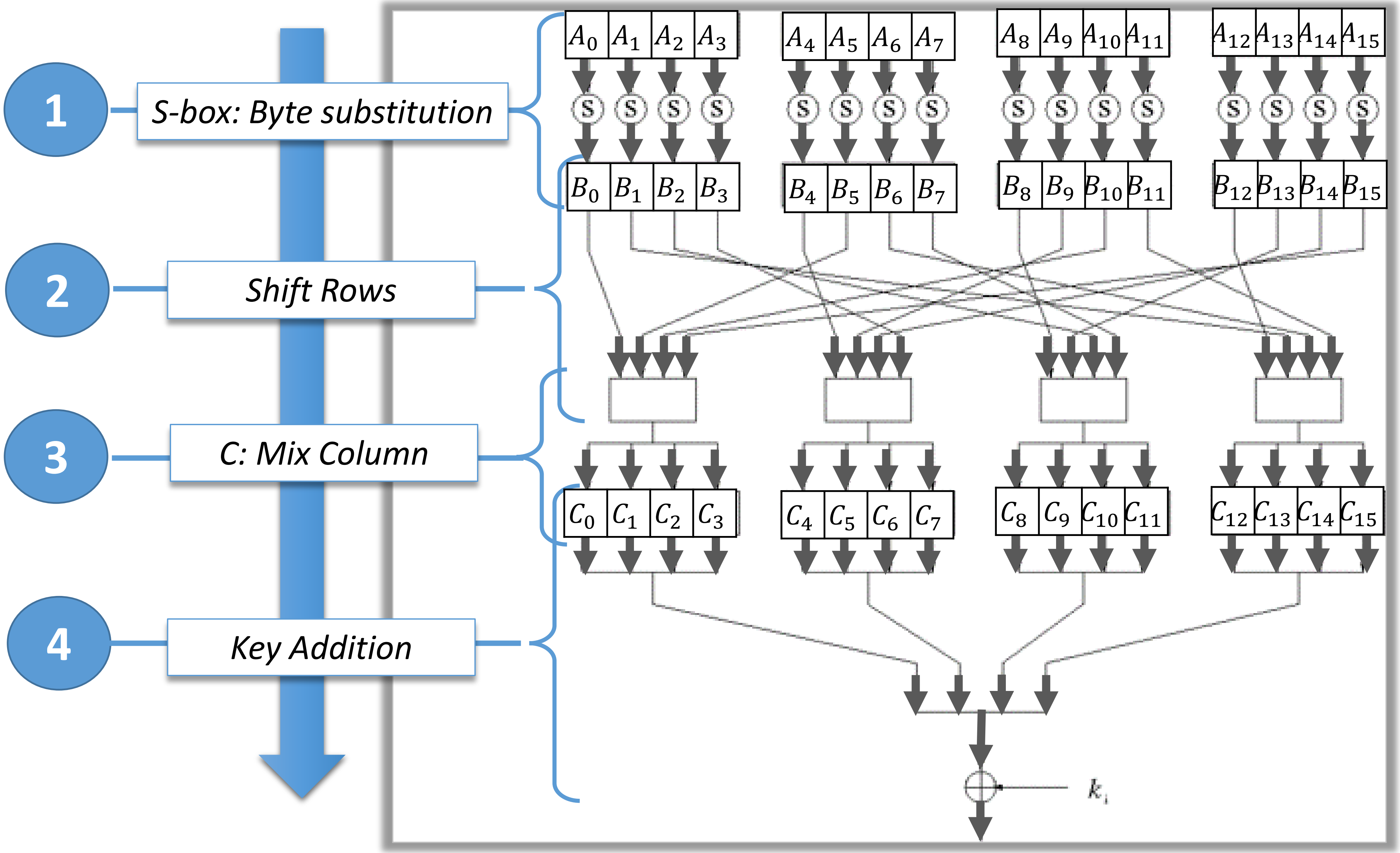
4 steps per round (not the last one)

1. Substitution by byte (core of the encryption)
2. Shift rows (Transposition: re-arrange)
3. Mix Columns (Substitution &Transposition)
4. Add round key (XOR)

3 steps for the last round

1. Substitution by byte (core of the encryption)
2. Shift rows (Transposition: re-arrange)
3. Mix Columns (Substitution &Transposition)
4. Add round key (XOR)

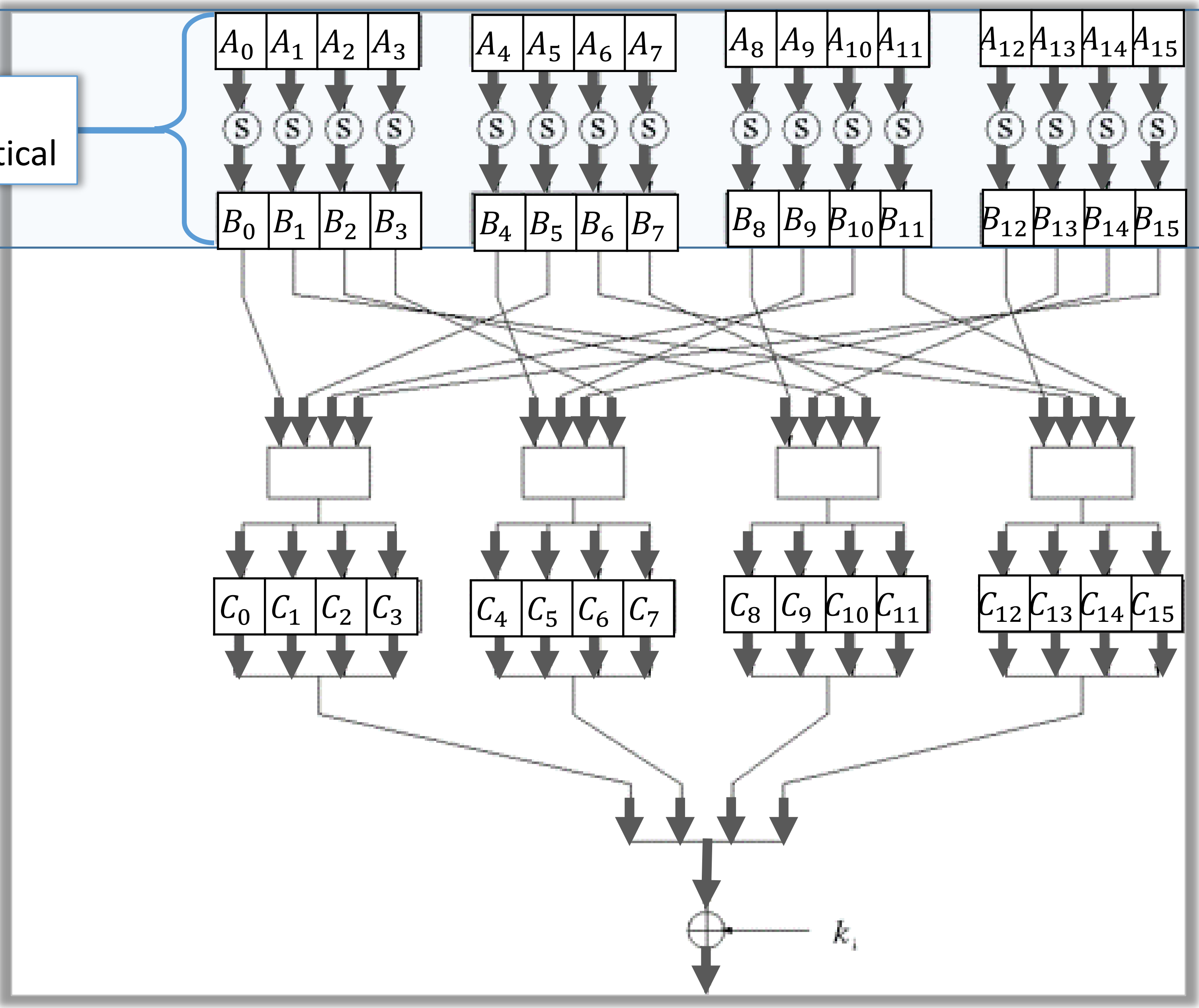
AES: description of each round



AES: step-1: Byte substitution; the s-boxes

1

$A_i \rightarrow B_i$ = S (A_i)
All 16 S-boxes are identical



Description of byte substitution S-box – base 16

$A_i = x\ y$

$B_i = S(A_i)$

$A_i = C\ 2$

	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

$B_i = 2\ 5$

0000	0
0001	1
0010	2
0011	3
0100	4
0101	5
0110	6
0111	7
1000	8
1001	9
1010	a
1011	b
1100	c
1101	d
1110	e
1111	f

Example: [A_i = 1100 0010 = *C 2*] => [B_i = *2 5* = 0010 0101]

Construction of the byte substitution S-box

1- Conversion to Galois field vector:

(Input bit vector is transformed into a polynomial vector)

$$A_i = \{a_{7i}; a_{6i}; a_{5i}; a_{4i}; a_{3i}; a_{2i}; a_{1i}; a_{0i}\}$$

$$\rightarrow A_i(X) = a_{7i} X^7 + a_{6i} X^6 + a_{5i} X^5 + a_{4i} X^4 + a_{3i} X^3 + a_{2i} X^2 + a_{1i} X + a_{0i}$$

for $n \in \{0, 7\}$: $a_{ni} \in \{0,1\}$

2- Find the Galois field inverse of $A_i(X)$: $B_i'(X)$

$B_i'(X) = A_i(X)^{-1}$ see table

$A_i(X) \times B_i'(X) \equiv 1 \bmod P(X)$; $P(X)$ is the $GF2^8$ irreducible polynomial:

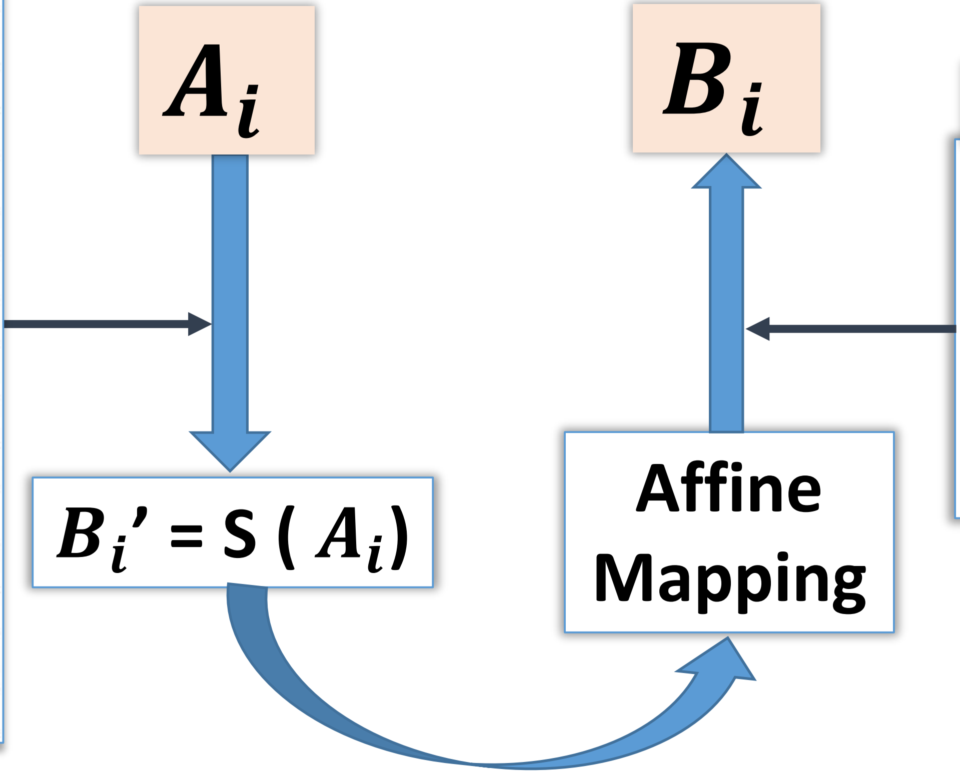
$$P_{(x)} = x^8 + x^4 + x^3 + x + 1$$

3- Extract B_i from B_i' from the "Affine Mapping" see table

Example: Construction of the byte substitution S-box

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

Find the Inverse



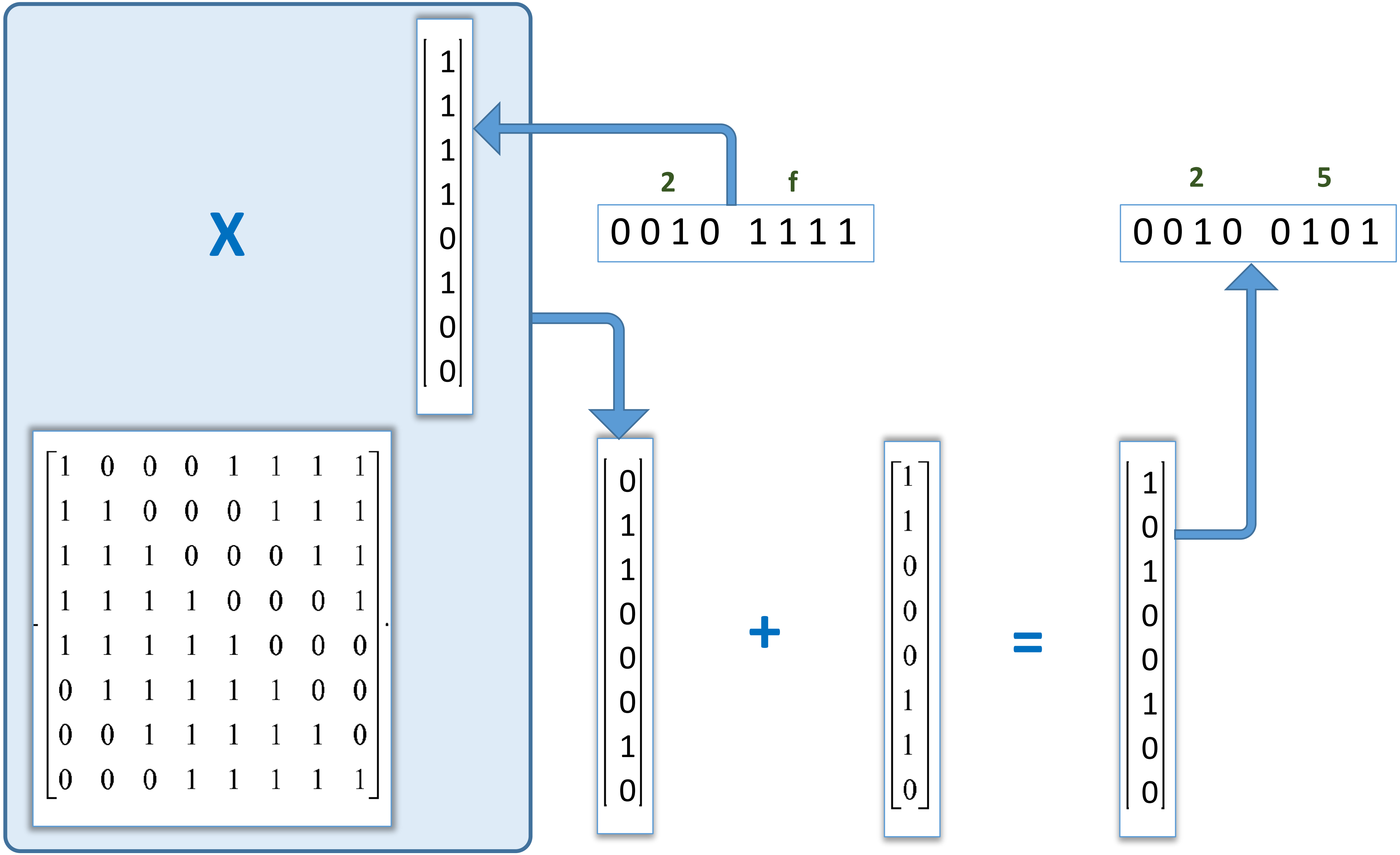
B_i $\qquad\qquad$ B_i'

$$\begin{bmatrix} y_0\\ y_1\\ y_2\\ y_3\\ y_4\\ y_5\\ y_6\\ y_7 \end{bmatrix} \leftarrow \begin{bmatrix} 1&0&0&0&1&1&1&1\\ 1&1&0&0&0&1&1&1\\ 1&1&1&0&0&0&1&1\\ 1&1&1&1&0&0&0&1\\ 1&1&1&1&1&0&0&0\\ 0&1&1&1&1&1&0&0\\ 0&0&1&1&1&1&1&0\\ 0&0&0&1&1&1&1&1 \end{bmatrix} \cdot \begin{bmatrix} x_0\\ x_1\\ x_2\\ x_3\\ x_4\\ x_5\\ x_6\\ x_7 \end{bmatrix} + \begin{bmatrix} 1\\ 1\\ 0\\ 0\\ 0\\ 1\\ 1\\ 0 \end{bmatrix}$$

Matrix transform

<u>Example:</u>

$A_i = 1100\ 0010$ (c 2)	➔ $B_i' = 0010\ 1111$ (2 f)	➔ $B_i = 0010\ 0101$ (2 5)
$A_i(X) = X^7 + X^6 + X$	➔ $B_i'(X) = X^5 + X^3 + X^2 + X + 1$	➔ $B_i(X) = X^5 + X^2 + 1$

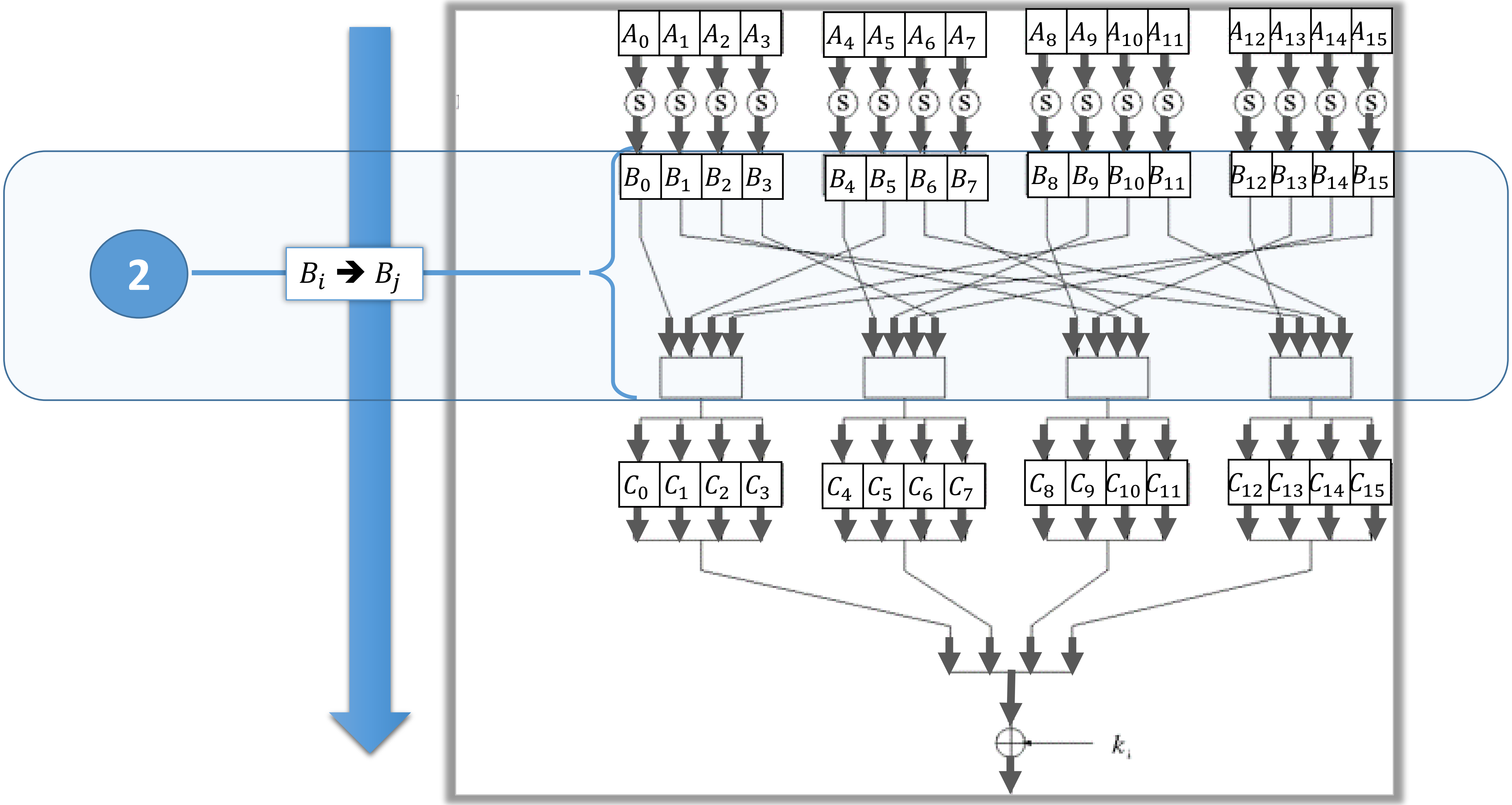

X
2
f
0 0 1 0 1 1 1 1
2
5
0 0 1 0 0 1 0 1
+
=

Homework 4-A

Find B'i, the inverse of Ai with GF, and Bi after affine mapping

A_i	B'_i	B_i
0101 1000		
1101 0001		
1011 1010		
1110 0011		
0110 1000		

AES step -2: Shift Rows



AES step -2: Shift Rows

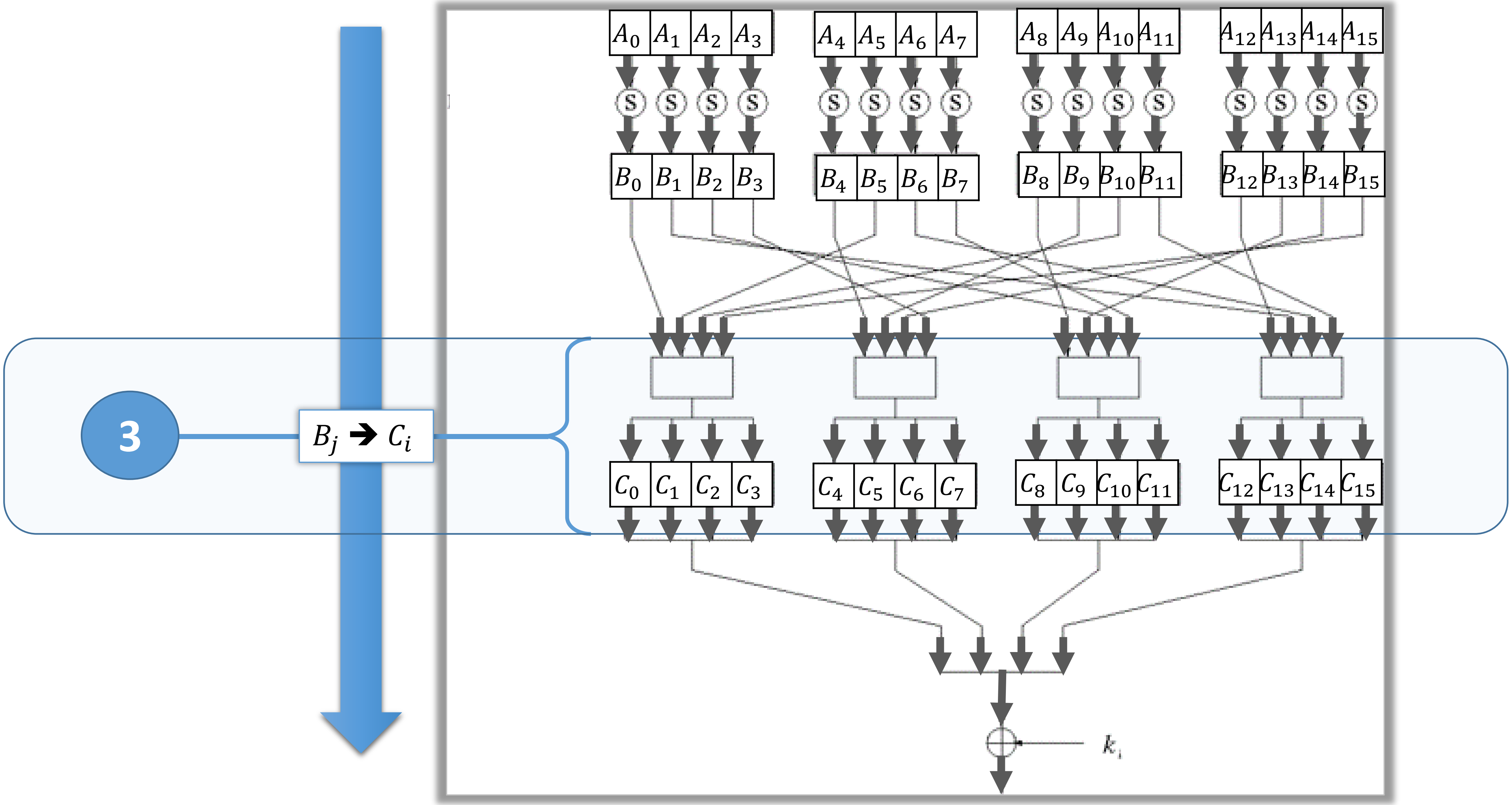
B_0	B_4	B_8	B_{12}
B_1	B_5	B_9	B_{13}
B_2	B_6	B_{10}	B_{14}
B_3	B_7	B_{11}	B_{15}

Input matrix

B_0	B_4	B_8	B_{12}	*No shift*
B_5	B_9	B_{13}	B_1	*one left*
B_{10}	B_{14}	B_2	B_6	*two left*
B_{15}	B_3	B_7	B_{11}	*Three left*

output matrix

AES step-3: Mix Column



AES step-3: Mix columns transformation

B_0	B_5	B_{10}	B_{15}
MIX			
C_0	C_1	C_2	C_3

B_4	B_9	B_{14}	B_3
MIX			
C_4	C_5	C_6	C_7

B_8	B_{13}	B_2	B_7
MIX			
C_8	C_9	C_{10}	C_{11}

B_{12}	B_1	B_6	B_{11}
MIX			
C_{12}	C_{13}	C_{14}	C_{15}

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

$$\begin{pmatrix} C_4 \\ C_5 \\ C_6 \\ C_7 \end{pmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{pmatrix} B_4 \\ B_9 \\ B_{14} \\ B_3 \end{pmatrix}$$

$$\begin{pmatrix} C_8 \\ C_9 \\ C_{10} \\ C_{11} \end{pmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{pmatrix} B_8 \\ B_{13} \\ B_2 \\ B_7 \end{pmatrix}$$

$$\begin{pmatrix} C_{12} \\ C_{13} \\ C_{14} \\ C_{15} \end{pmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{pmatrix} B_{12} \\ B_1 \\ B_6 \\ B_{11} \end{pmatrix}$$

Galois Fields matrix transform – Example:

$C_0 = [[02] \cdot B_0] \oplus [[03] \cdot B_5] \oplus [[01] \cdot B_{10}] \oplus [[01] \cdot B_{15}]$

$C_1 = [[01] \cdot B_0] \oplus [[02] \cdot B_5] \oplus [[03] \cdot B_{10}] \oplus [[01] \cdot B_{15}]$

$C_2 = [[01] \cdot B_0] \oplus [[01] \cdot B_5] \oplus [[02] \cdot B_{10}] \oplus [[03] \cdot B_{15}]$

$C_3 = [[03] \cdot B_0] \oplus [[01] \cdot B_5] \oplus [[01] \cdot B_{10}] \oplus [[02] \cdot B_{15}]$

Maths: Extended Galois field

- 01 ➔ (0000 0001) ➔ 1
- 02 ➔ (0000 0010) ➔ x
- 03 ➔ (0000 0011) ➔ $x + 1$

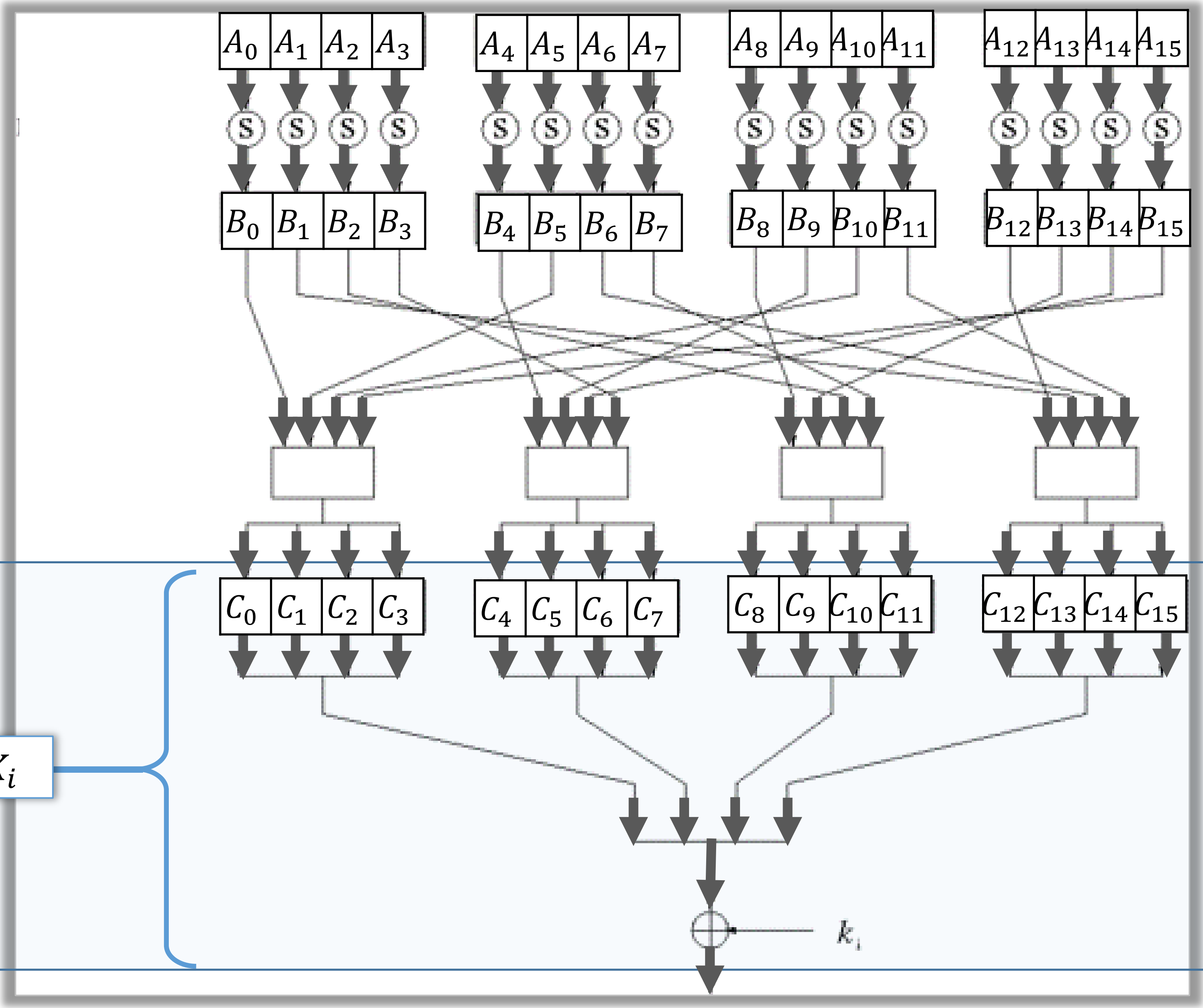
$$P_{(x)} = x^8 + x^4 + x^3 + x + 1$$

Homework 4-B

Find C_0, C_1, C_2, C_3 from B_0, B_5, B_{10}, C_{15} with mix column transform

B_0	B_5	B_{10}	B_{15}
0101 1000	1101 0001	1011 1010	1110 0011
C_0	C_1	C_2	C_3
?	?	?	?

AES step-4: Key addition (XOR)



4

$C_i \rightarrow C'_i = C_i \oplus K_i$

AES step-4: Key addition - Add Round key

- Operation done before the first round, then at every round
- At round i the key generated by the key processor is different
- The key $\boldsymbol{K_i}$ is segmented by byte:

$$\boldsymbol{K_i} = \{\boldsymbol{K_{1i}}; \boldsymbol{K_{2i}}; \ldots; \boldsymbol{K_{ji}}; \ldots; \boldsymbol{K_{16i}}\}$$

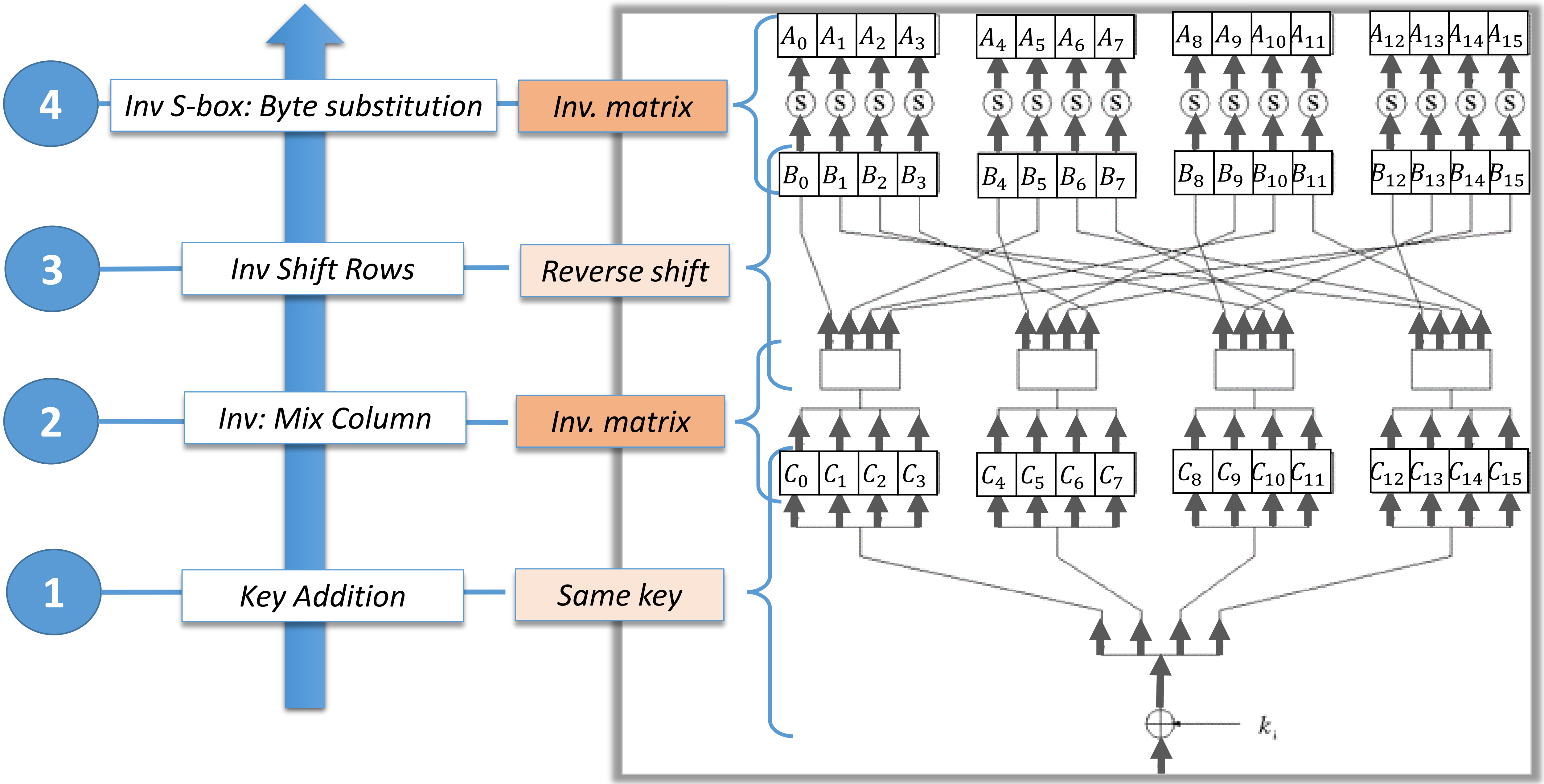
- Assuming that the plain text is $\boldsymbol{P_i}$:

$$\boldsymbol{P_i} = \{\boldsymbol{P_{1i}}; \boldsymbol{P_{2i}}; \ldots; \boldsymbol{P_{ji}}; \ldots; \boldsymbol{P_{16i}}\}$$

- The encrypted text has also 16 bytes with $\boldsymbol{P'_{ji}}$ given by:

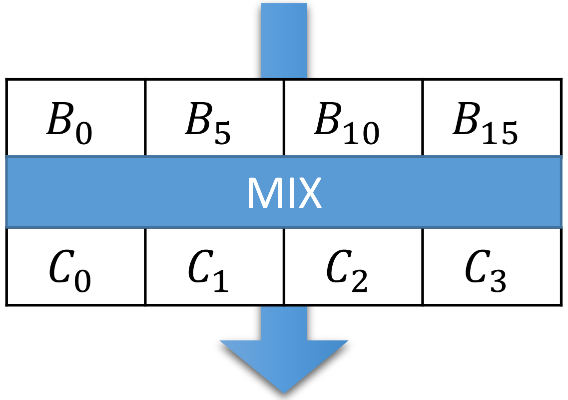
$$\boldsymbol{P'_{ji}} = \{\boldsymbol{P_{ji}} \oplus \boldsymbol{K_{ji}}\}$$

AES Inverse: decryption



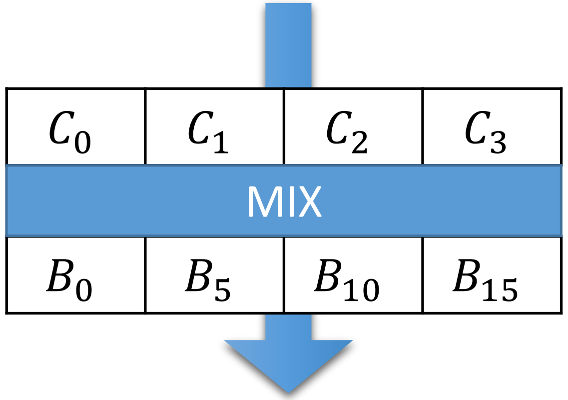
Inverse Mix columns transformation

Encrypt



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

Decrypt



$$\begin{pmatrix} B_0 \\ B_5 \\ B_{10} \\ B_{15} \end{pmatrix} = \begin{bmatrix} 0E & 0B & 0D & 09 \\ 09 & 0E & 0B & 0D \\ 0D & 09 & 0E & 0B \\ 0B & 0D & 09 & 0E \end{bmatrix} \begin{pmatrix} C_0 \\ C_1 \\ C_2 \\ C_3 \end{pmatrix}$$

Inverse S-Box

$\boldsymbol{B_i = x\ y}$

$\boldsymbol{A_i = S(A_i)}$

$\boldsymbol{B_i = C\ 2}$

		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

0000	0
0001	1
0010	2
0011	3
0100	4
0101	5
0110	6
0111	7
1000	8
1001	9
1010	a
1011	b
1100	c
1101	d
1110	e
1111	f

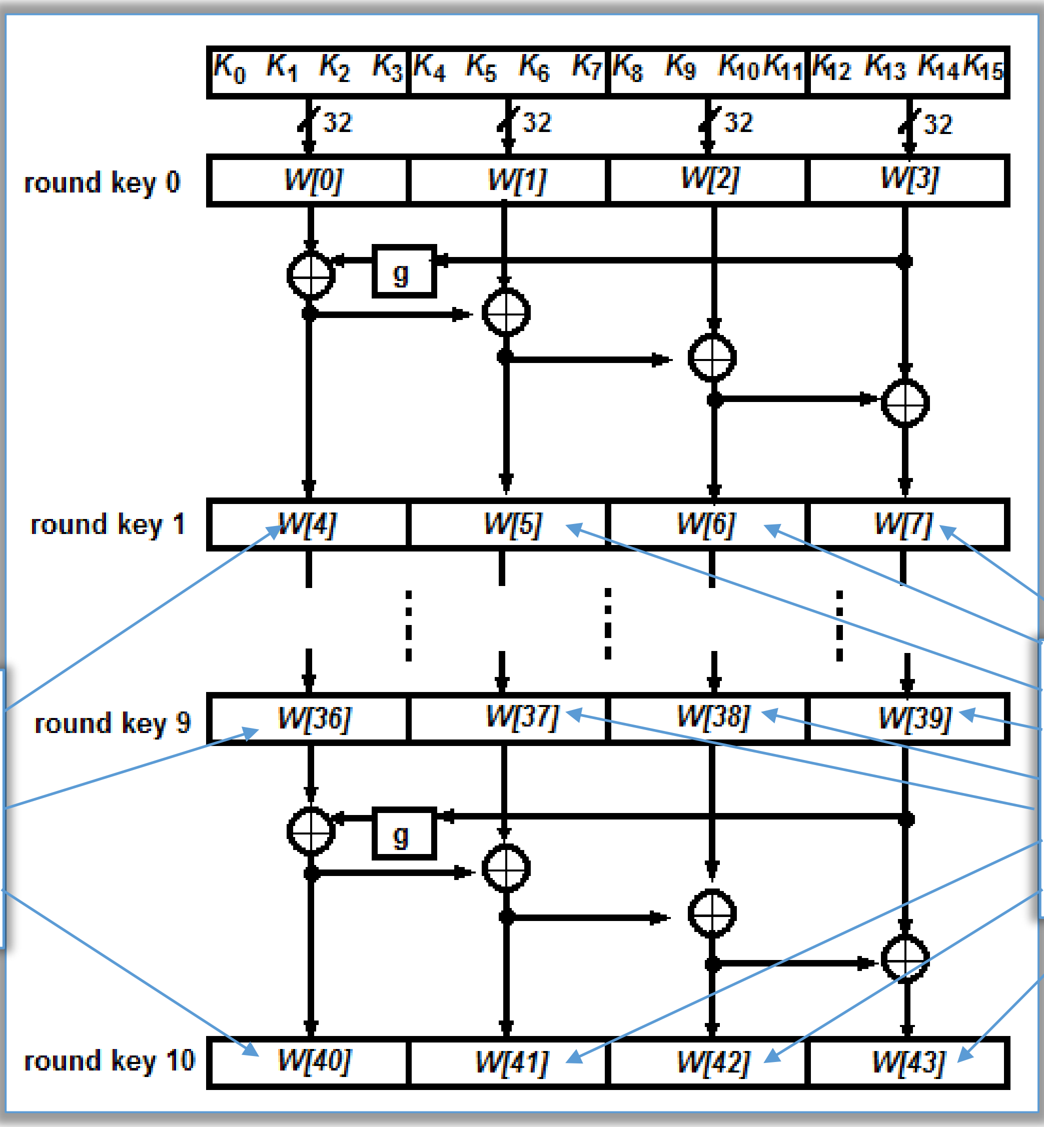
$\boldsymbol{A_i = A\ 8}$

Example: [B_i= 1100 0010 = *C 2*] => [A_i = *A 8* = 1010 1000]

Advanced Encryption Standard

- 1- Finite fields
- 2- Extended Galois fields
- 3- AES architecture
- 4- AES Key generation
- 5- Summary

AES: Key schedule for each round for 128-bit size



For the left-more word of sub-key

$i \in \{1 \text{ to } 10\}$

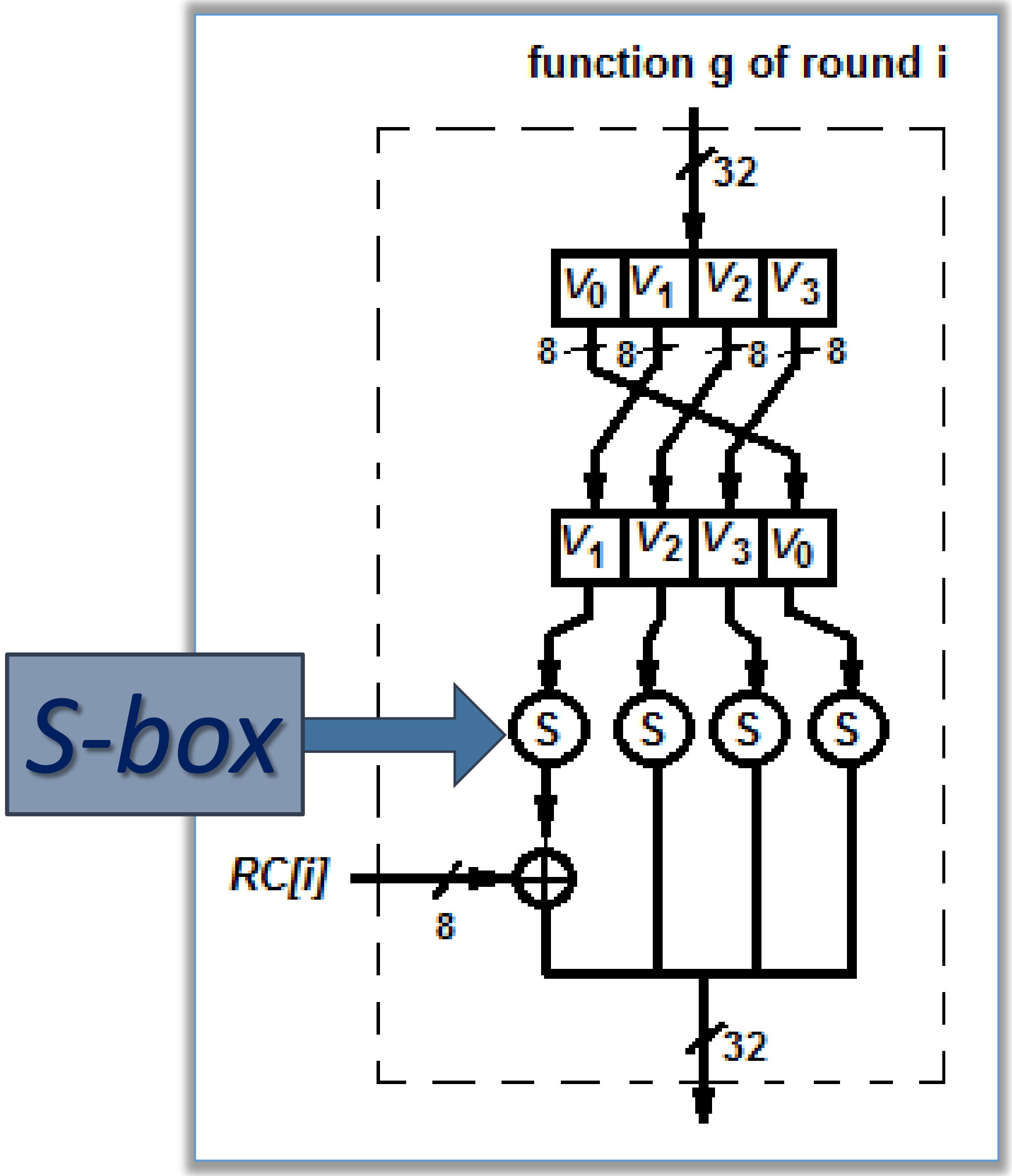
$W(4i) = W(4(i-1)) \oplus g(W(4i-1))$

For the other 3 words of sub-key

i ; $j = 1,2,3$

$W(4i+j) = W(4(i-1)+j) \oplus (W(4i+j-1))$

AES: Function g of round i



RC [1] = x^0 = (0000 0001)
RC [2] = x^1 = (0000 0010)
RC [3] = x^2 = (0000 0100)
RC [4] = x^3 = (0000 1000)
RC [5] = x^4 = (0001 0000)
RC [6] = x^5 = (0010 0000)
RC [7] = x^6 = (0100 0000)
RC [8] = x^7 = (1000 0000)
RC [9] = x^8 = (0001 1011)
RC[10] = x^9 = (0011 0110)

x^8= P(x)+RC[9]= $(x^8+x^4+x^3+x+1)+(x^4+x^3+x^1+1)$

x^9= xP(x)+RC[10]= $x(x^8+x^4+x^3+x+1)+(x^5+x^4+x^2+x)$

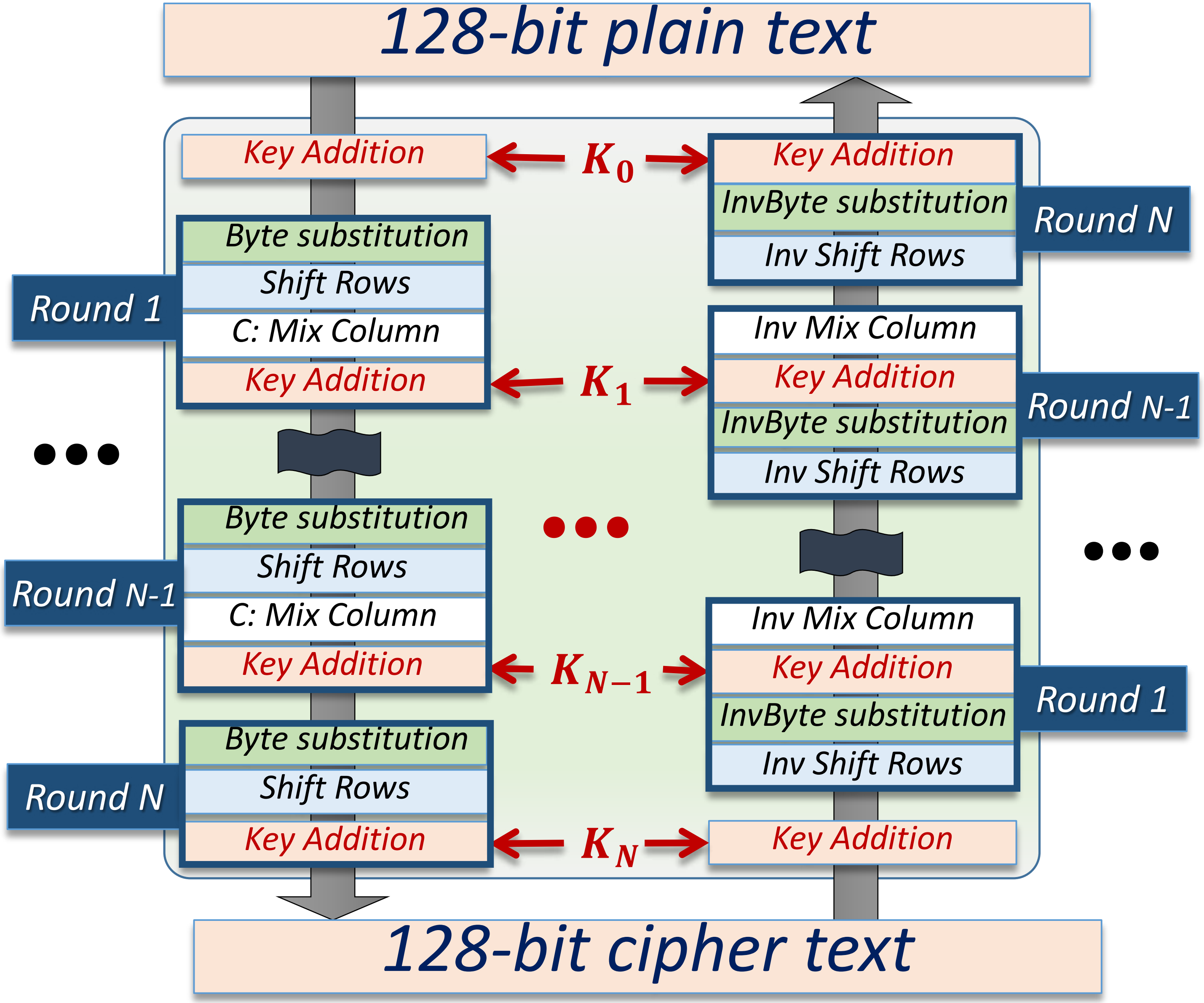
Advanced Encryption Standard

- 1- Finite fields
- 2- Extended Galois fields
- 3- AES architecture
- 4- AES Key generation
- 5- Summary

Summary: AES

- **Add round key – XOR (128 bits)**
- **10-12-14 rounds of encryption (128bits)**
  - Substitute Bytes S-boxes (Galois field)
  - Shift Row
  - Mixed Columns – not in last round
  - Add round key – XOR
- **Key processor:**
  - Key size 128 – 192 – 256
  - Create 32-bit words from four bytes
  - Each round key: XOR with a g-function
- **Reverse order for decryption**

N	size
10	128
12	192
14	256



Effect of fault injection on AES → not easy

- **Plaintext:** *32 43 f6 a8 88 5a 30 8d 31 31 98 a2 e0 37 07 34*
  128-bit key: *2b 7e 15 16 28 ae d2 a6 ab f7 15 88 09 cf 4f 3c*
  Ciphertext: *39 25 84 1d 02 dc 09 fb dc 11 85 97 19 6a 0b 32*

- **One fault in the plaintext:** *3**0** 43 f6 a8 88 5a 30 8d 31 31 98 a2 e0 37 07 34*
  Results in the ciphertext: ***c0 06 27 d1 8b d9 e1 19 d5 17 6d bc ba 73 37 c1***

- **One fault in the key:** *2**a** 7e 15 16 28 ae d2 a6 ab f7 15 88 09 cf 4f 3c*
  Results in the ciphertext: ***c4 61 97 9e e4 4d e9 7a ba 52 34 8b 39 9d 7f 84***

A single-bit error results in a totally scrambled output

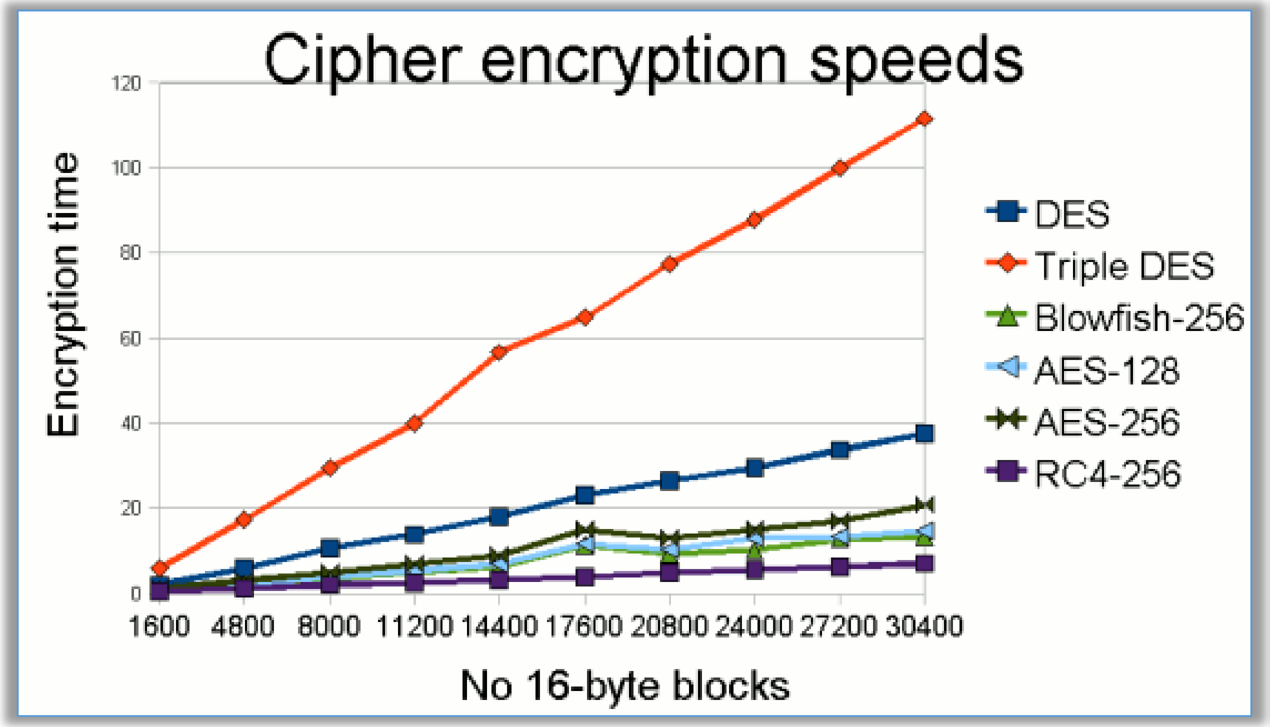
Comparing symmetrical methods

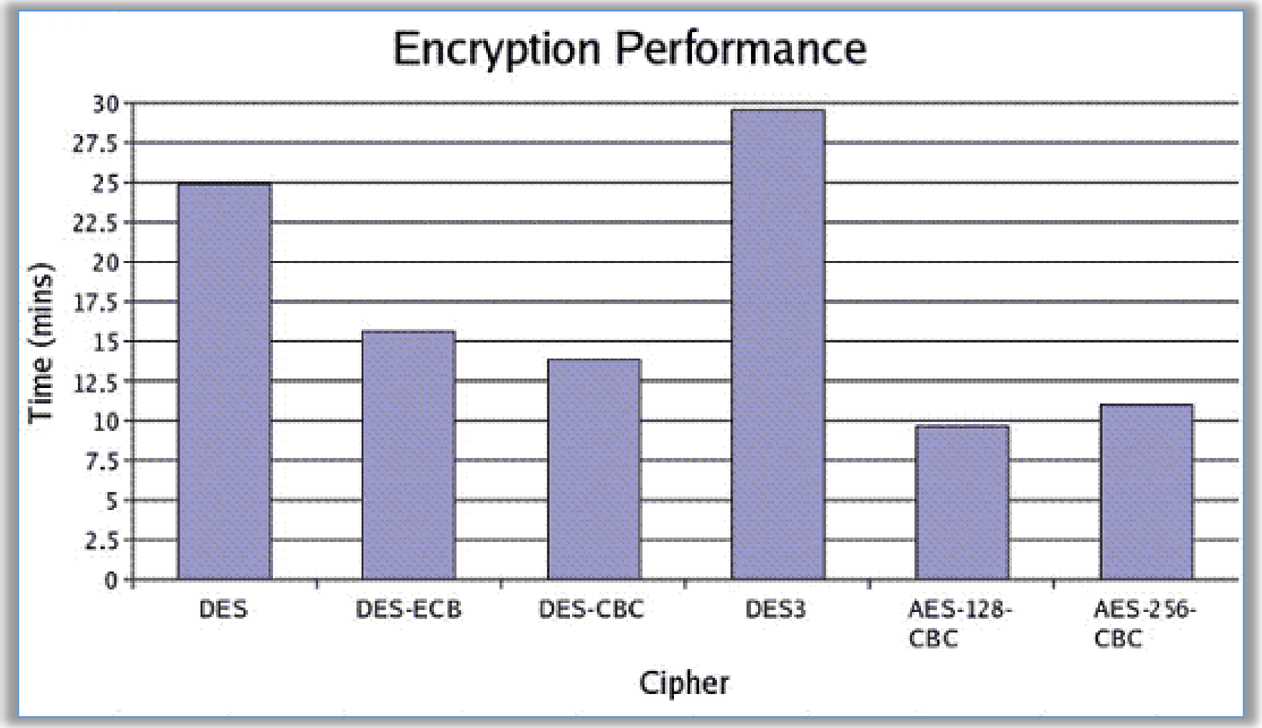
DES vs AES

	DES	AES
Date	1976	1999
Block size	64	128
Key length	56	128, 192, 256
Number of rounds	16	10, 12, 14
Encryption primitives	Substitution, permutation	Substitution, shift, bit mixing
Cryptographic primitives	Confusion, diffusion	Confusion, diffusion
Design	Open	Open
Design rationale	Closed	Open
Selection process	Secret	Secret, but accept open public comment
Source	IBM, enhanced by NSA	Independent cryptographers

Form	Properties	Strength
DES	One 56-bit key	Weak
Double DES	Two 56-bit keys	2 X as strong as DES
Two-Key Triple DES	Two 56-bit keys	16 million times as strong as DES
Three-Key Triple DES	Three 56-bit keys	10^{17} as strong as DES
AES	128-bit key	4 10^{21} as strong as DES

Comparing cryptographic methods





Issues with AES

- **Almost 20 year old**
- **Sensitive to frequency analysis**
  - Plain text is encrypted 128 bit at the time with the same key
  - Very long plain text give an opportunity to crypto-analyst
- **Collisions were reported on the Keys:**
  - Key size of 128 bits → 64 bits **Not safe**
  - Key size of 256 bits → 128 bits **Questionable**
- **Alternate encryption methods based on chaos, and random elements**

QUESTIONS ?

Dr. Bertrand Cambou
Professor of Practice NAU, Cybersecurity
School of Informatics, Computing, and Cyber-Systems
Bertrand.cambou@nau.edu