Computer Network Security

TE - IT

Lecture -11
04/08/2022

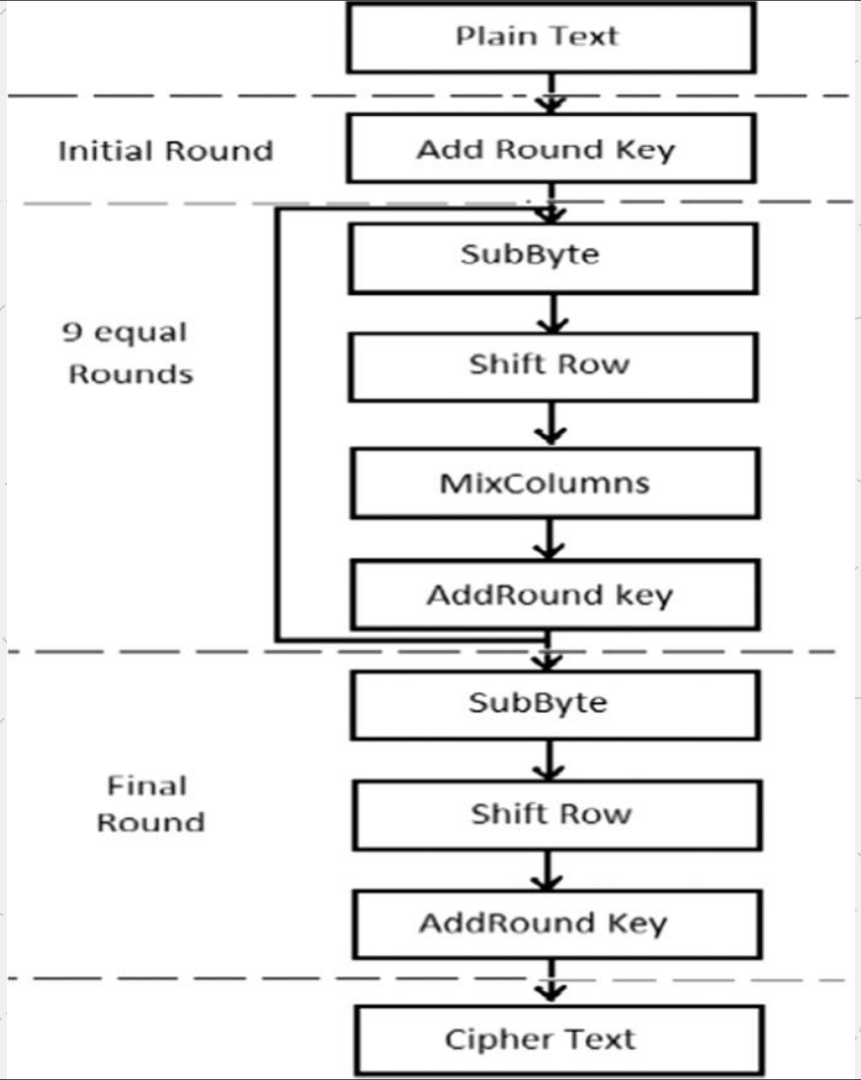
Session: 9:45 - 10:45 AM

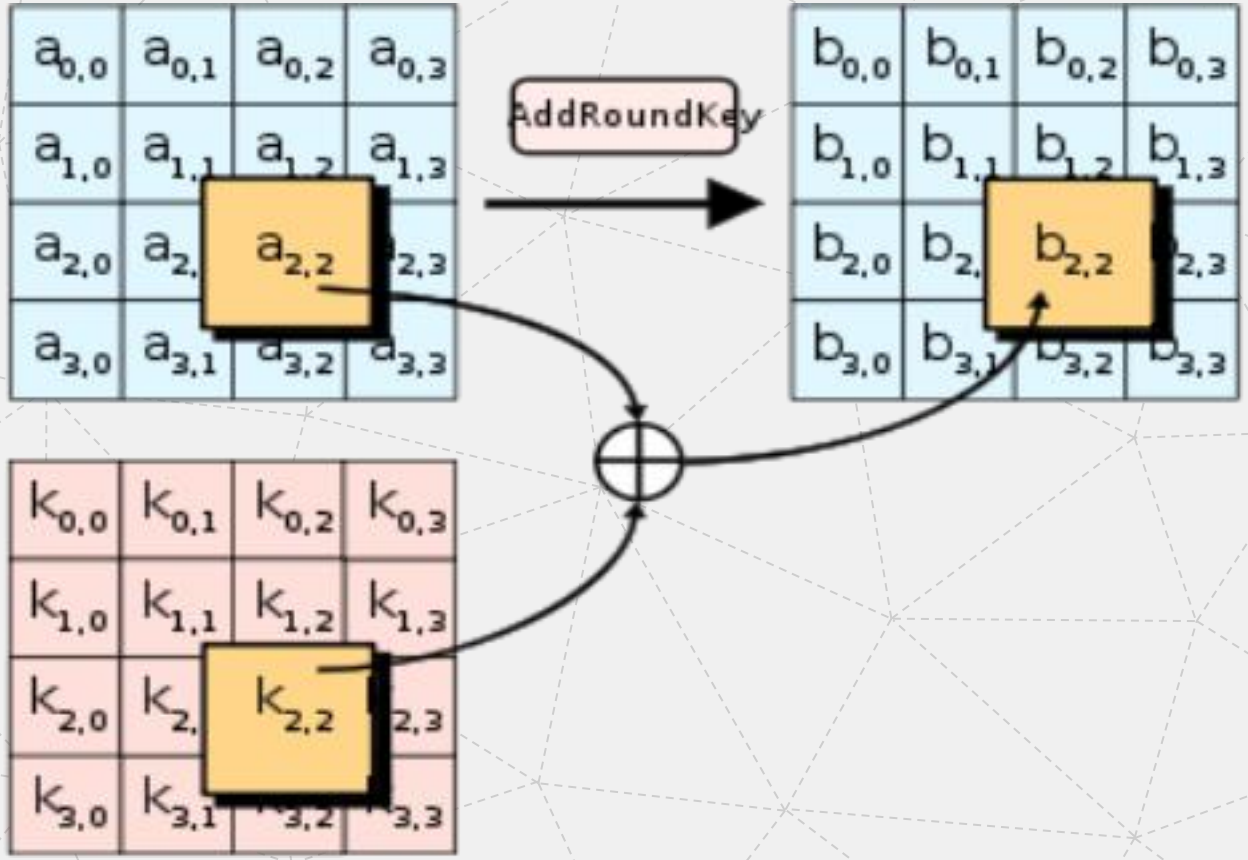
Prof. Stella J
Department of Information Technology
Xavier Institute of Engineering

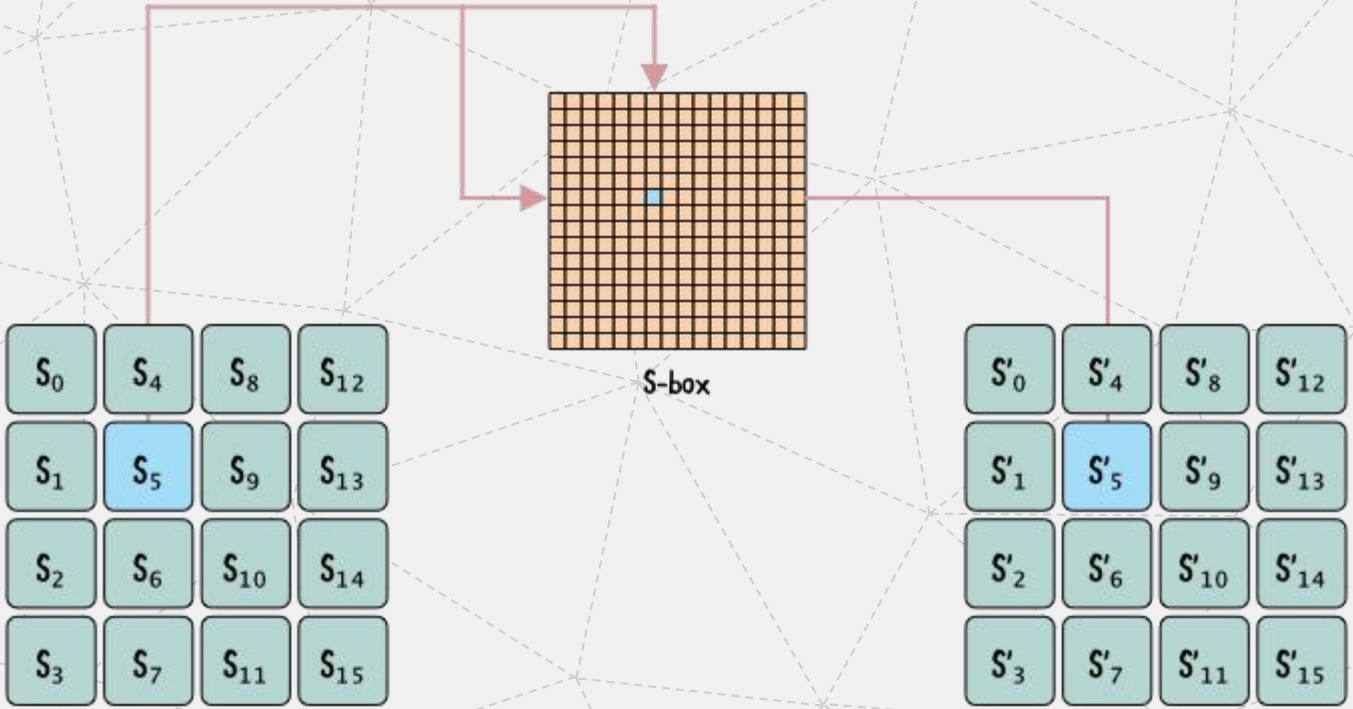
Module-2

- ✓ AES

AES Algorithm Architecture:

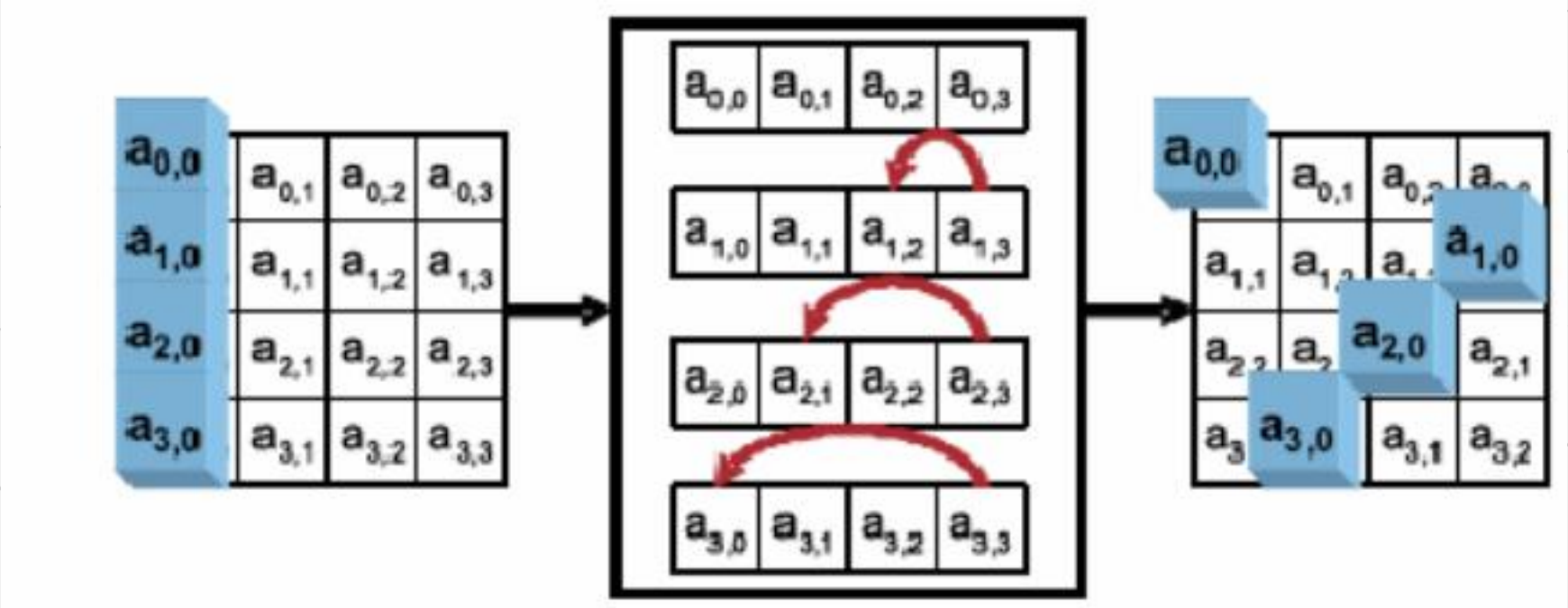



AddRoundKey

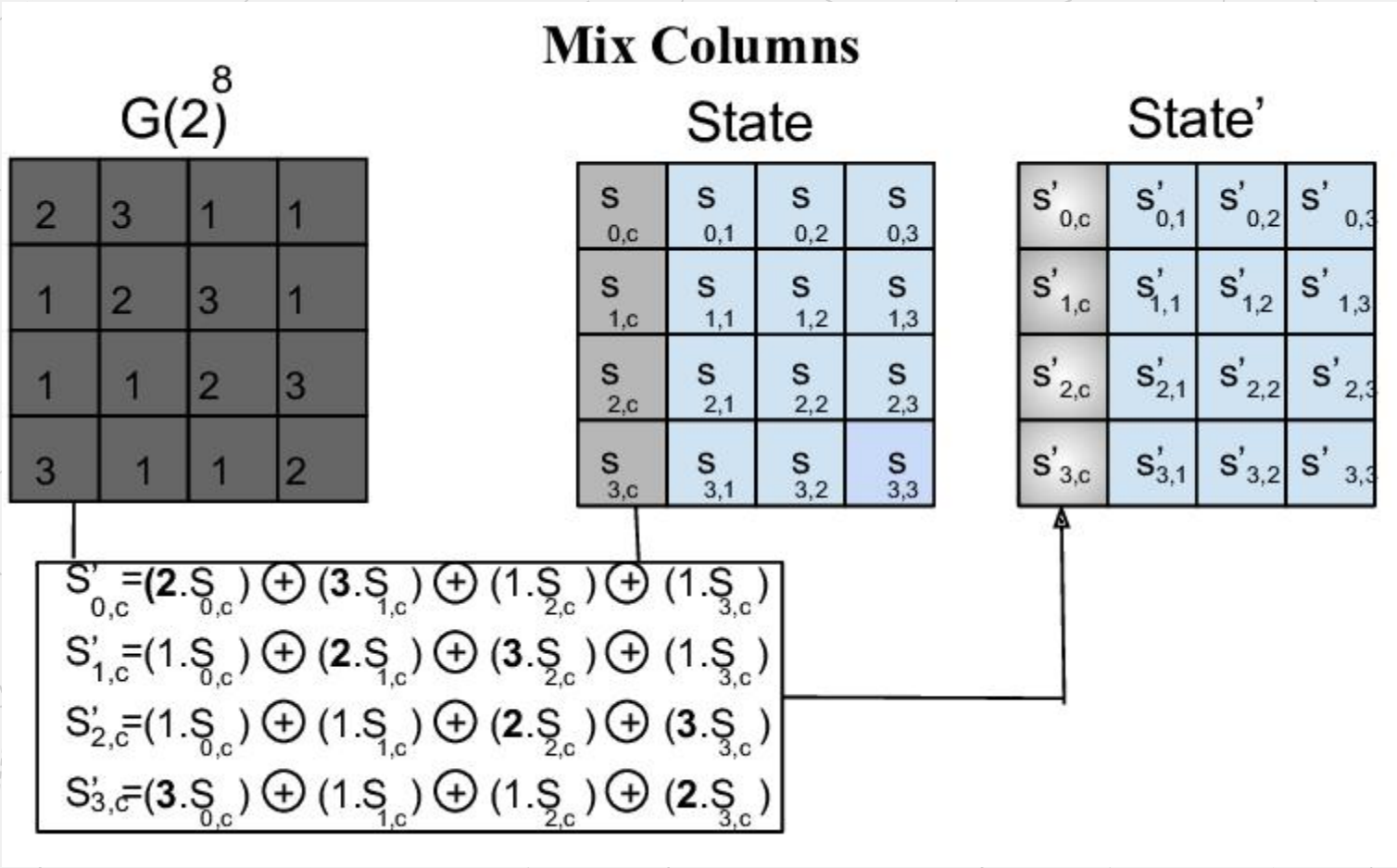

S0 S4 S8 S12
S1 S5 S9 S13
S2 S6 S10 S14
S3 S7 S11 S15
S-box
S'0 S'4 S'8 S'12
S'1 S'5 S'9 S'13
S'2 S'6 S'10 S'14
S'3 S'7 S'11 S'15

S - BOX

X \ Y	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	45	06	B0	E3	EB	27	16	43	46	47	74	34	B8	1F	12	FC
1	C4	B5	10	4A	89	F2	FD	73	BB	CB	3C	23	BA	95	CD	3E
2	85	6C	3D	2B	EF	C1	96	6D	77	DA	CA	3F	19	98	0A	B2
3	39	DB	56	EA	AD	40	76	13	EE	57	2D	2F	01	67	F8	28
4	25	F9	D1	35	79	5A	26	94	44	F0	53	B4	AC	63	05	1C
5	08	B6	B	98	82	20	2C	69	6B	88	AB	68	E2	4B	BE	B9
6	FA	30	5E	C5	CC	07	92	50	65	5D	93	D2	DC	15	6E	C6
7	90	70	18	AA	71	F6	24	0E	33	C9	00	CE	CF	F4	A7	62
8	21	58	16	E4	5B	C	29	2A	0F	41	9E	59	A0	C3	E1	81
9	91	61	9F	A9	1A	78	E9	4F	B1	7C	02	FE	31	17	BD	4C
A	B7	DE	BC	F1	36	A2	B3	8F	96	2E	F7	09	95	94	86	7B
B	52	5C	93	8E	32	87	D3	8A	C2	75	42	4D	EC	AF	6F	69
C	99	37	FF	49	9C	0D	51	97	D5	E5	64	48	AE	7F	9B	D7
D	55	8D	1D	38	7A	DF	DA	C0	DD	3B	39	4E	84	72	D0	22
E	FB	11	8B	83	BF	D4	E6	D8	5F	04	C8	99	F5	A1	E0	7D
F	7E	E8	03	14	E7	1E	80	F3	54	C7	96	8C	60	ED	D6	66


a0,0
a0,1
a0,2
a0,3
a1,0
a1,1
a1,2
a1,3
a2,0
a2,1
a2,2
a2,3
a3,0
a3,1
a3,2
a3,3

Mix Columns


G(2)^8
State
State'
2 3 1 1
1 2 3 1
1 1 2 3
3 1 1 2
s 0,c s 0,1 s 0,2 s 0,3
s 1,c s 1,1 s 1,2 s 1,3
s 2,c s 2,1 s 2,2 s 2,3
s 3,c s 3,1 s 3,2 s 3,3
s'0,c s'0,1 s'0,2 s'0,3
s'1,c s'1,1 s'1,2 s'1,3
s'2,c s'2,1 s'2,2 s'2,3
s'3,c s'3,1 s'3,2 s'3,3
S'0,c =(2.S0,c) ⊕ (3.S1,c) ⊕ (1.S2,c) ⊕ (1.S3,c)
S'1,c =(1.S0,c) ⊕ (2.S1,c) ⊕ (3.S2,c) ⊕ (1.S3,c)
S'2,c =(1.S0,c) ⊕ (1.S1,c) ⊕ (2.S2,c) ⊕ (3.S3,c)
S'3,c =(3.S0,c) ⊕ (1.S1,c) ⊕ (1.S2,c) ⊕ (2.S3,c)

THANK YOU