Classical Cryptography

Block ciphers: DES and AES

Karst Koymans

Informatics Institute

University of Amsterdam

(version 19.3, 2020/03/04 14:52:11 UTC)

Thursday, March 5, 2020

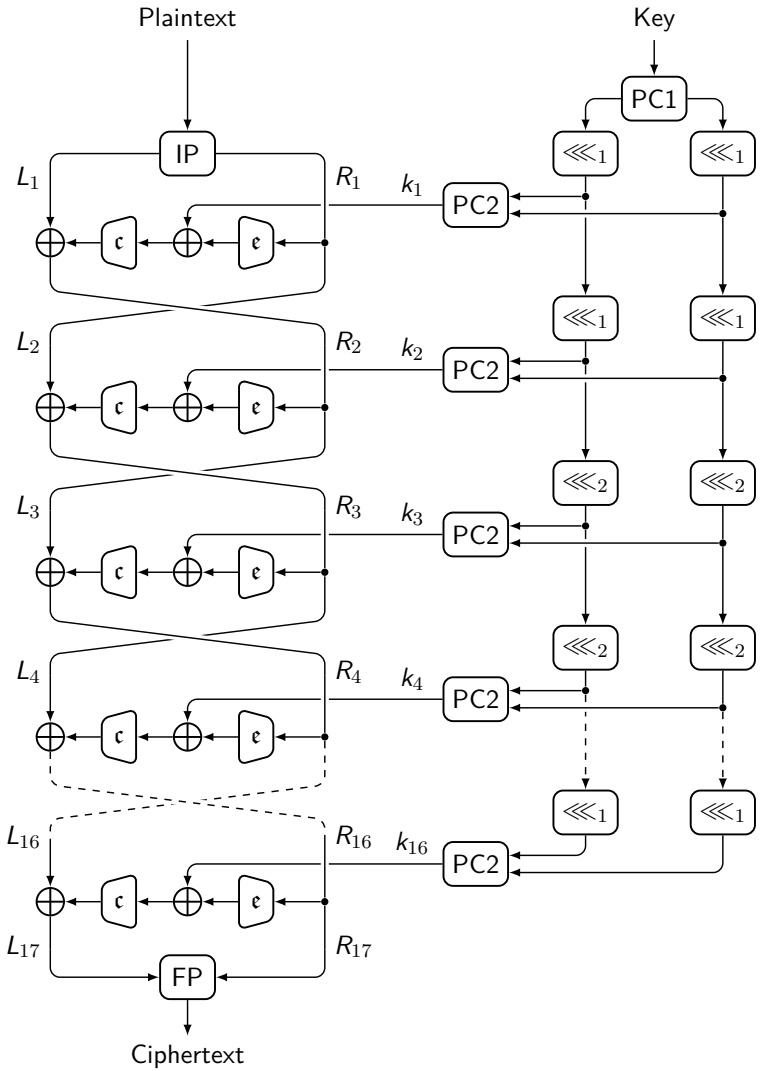
1. The Data Encryption Standard DES
2. The Advanced Encryption Standard AES

Outline

1 The Data Encryption Standard DES

2 The Advanced Encryption Standard AES

DES Overview



DES initial (IP) and final (FP) permutation

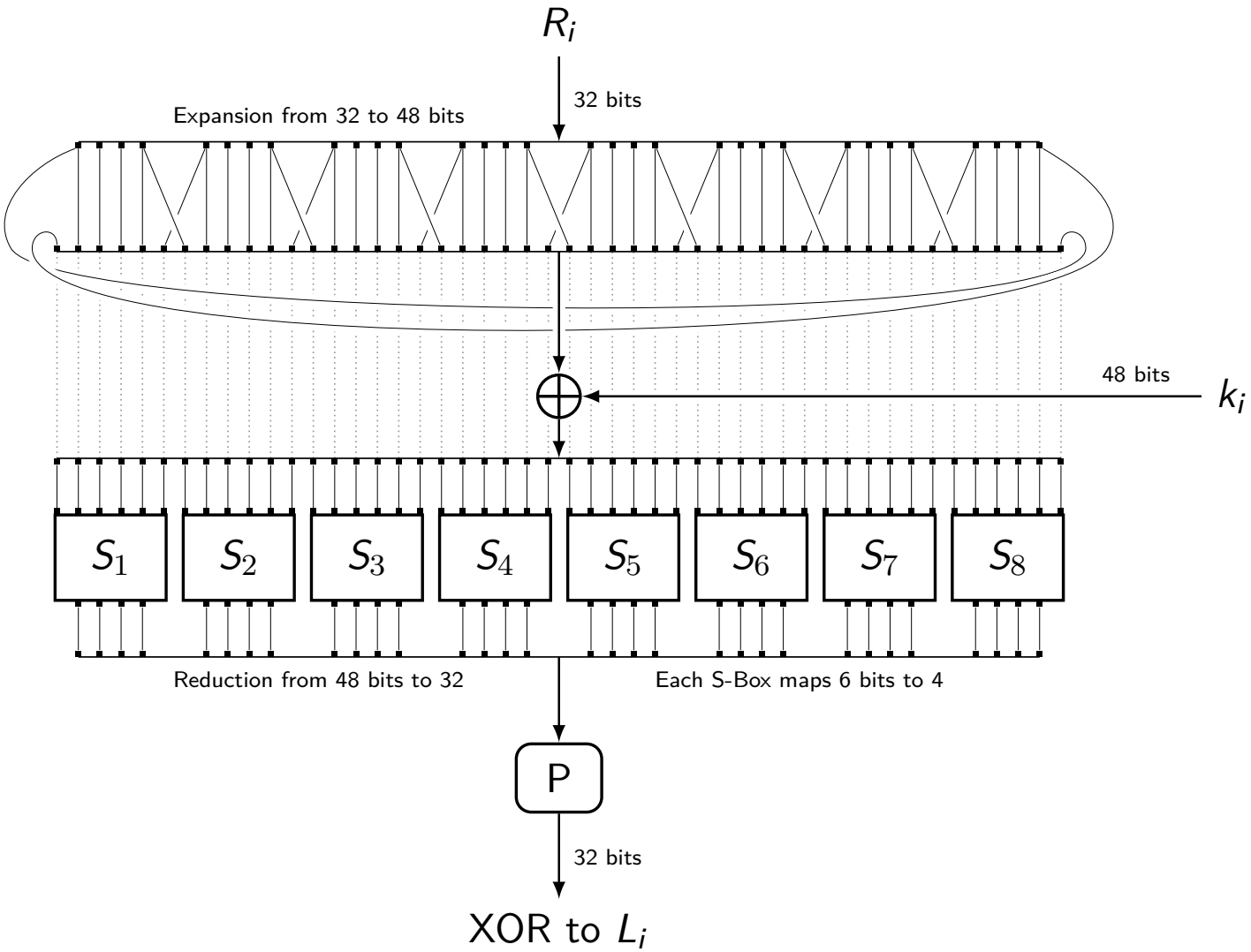
58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

Read this table row by row

For IP bit 58 moves to the first position

For FP bit 1 moves to position 58

DES round


R_i
32 bits
Expansion from 32 to 48 bits
48 bits
k_i
S_1
S_2
S_3
S_4
S_5
S_6
S_7
S_8
Reduction from 48 bits to 32
Each S-Box maps 6 bits to 4
P
32 bits
XOR to L_i

DES P-box permutation

16	7	20	21	29	12	28	17
1	15	23	26	5	18	31	10
2	8	24	14	32	27	3	9
19	13	30	6	22	11	4	25

DES PC1 (permuted choice 1)

57	49	41	33	25	17	9
1	58	50	42	34	26	18
10	2	59	51	43	35	27
19	11	3	60	52	44	36
63	55	47	39	31	23	15
7	62	54	46	38	30	22
14	6	61	53	45	37	29
21	13	5	28	20	12	4

Reduces from 64 bits to 56 bits by leaving out parity bits

DES PC2 (permuted choice 2)

14	17	11	24	1	5	3	28
15	6	21	10	23	19	12	4
26	8	16	7	27	20	13	2
41	52	31	37	47	55	30	40
51	45	33	48	44	49	39	56
34	53	46	42	50	36	29	32

Reduces from 56 bits to 48 bits leaving out bits

9, 18, 22, 25, 35, 38, 43, 54

Outline

1 The Data Encryption Standard DES

2 The Advanced Encryption Standard AES

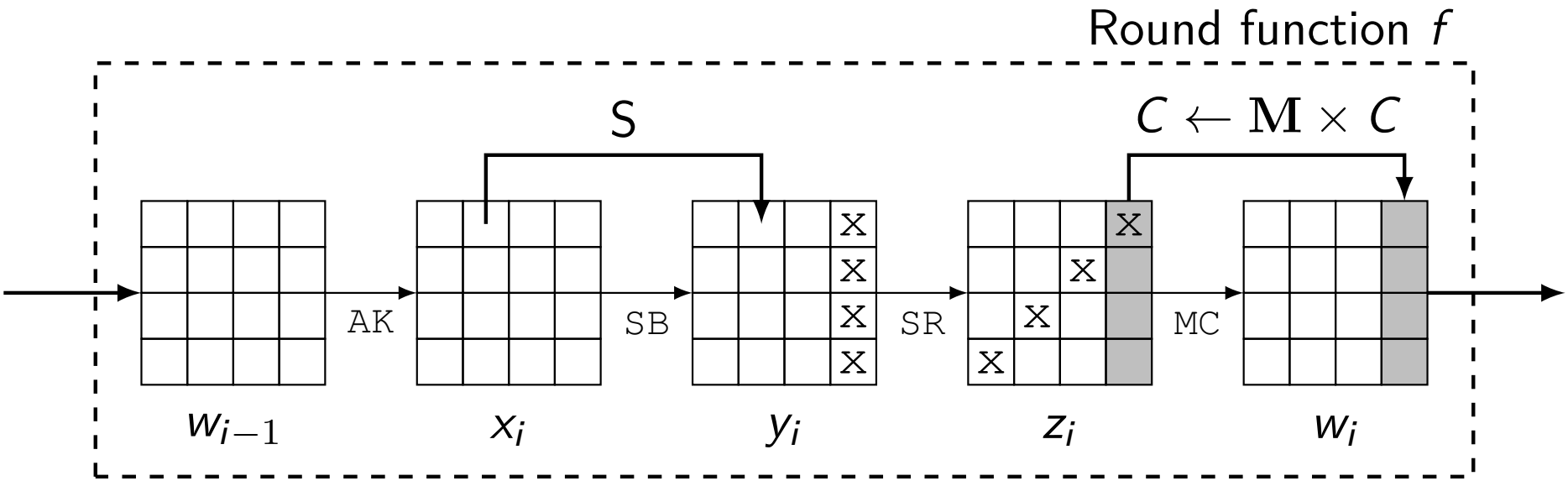
AES state

0	4	8	12
1	5	9	13
2	6	10	14
3	7	11	15

Each square represents one byte for a total of 128 bits

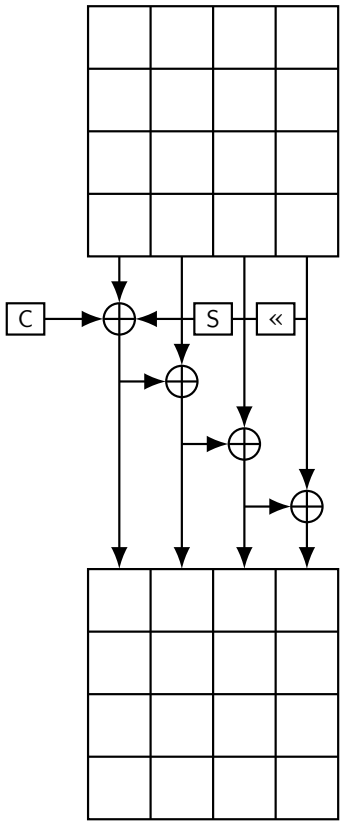
Each column represents a word consisting of 4 bytes

AES Overview



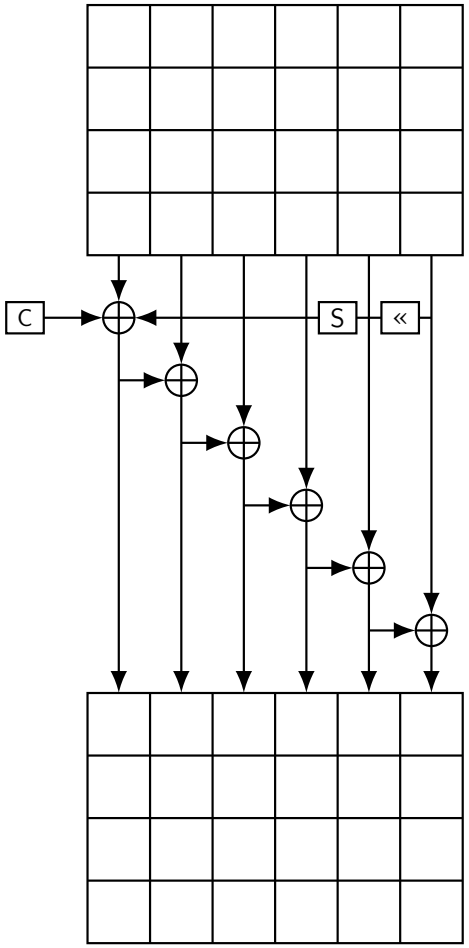
AK: Add Key, SB: Sub Bytes, SR: Shift Rows, MC: Mix Columns

AES key schedule (128 bit keys)

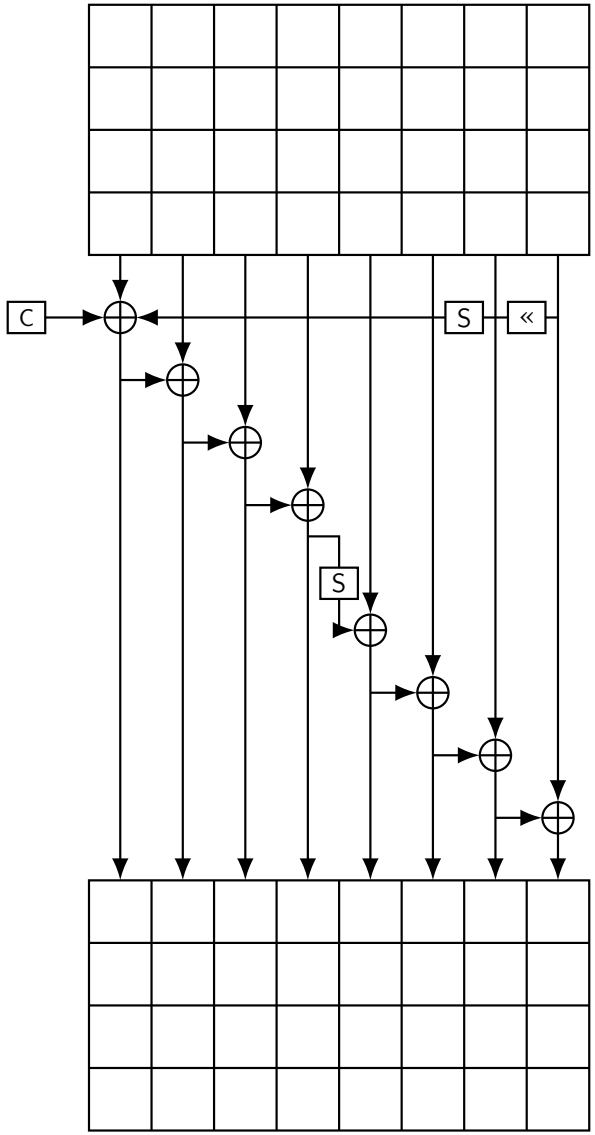


C: (Round dependent) Constant, S: Sub word, «: Rotate word

AES key schedule (192 bit keys)



AES key schedule (256 bit keys)



AES animation and stick guide

https://www.youtube.com/watch?v=gP4PqVGudtg

http://www.moserware.com/2009/09/

stick-figure-guide-to-advanced.html