Euclidean Algorithm

q	r_1	r_2	r
1	2740	1760	980
1	1760	980	780
1	980	780	200
3	780	200	180
1	200	180	20
9	180	20	0
	20	0	

Extended Euclidean Algorithm

q	r_1	r_2	r	s_1	s_2	s	t_1	t_2	t
5	161	28	21	1	0	1	0	1	-5
1	28	21	7	0	1	-1	1	-5	6
3	21	7	0	1	-1	4	-5	6	-23
	7	0		-1	4		6	-23	

DES

64-bit plaintext

Initial permutation

Round 1 K_1 48-bit

Round 2 K_2 48-bit

Round 16 K_{16} 48-bit

Round-key generator

56-bit cipher key

Final permutation

64-bit ciphertext
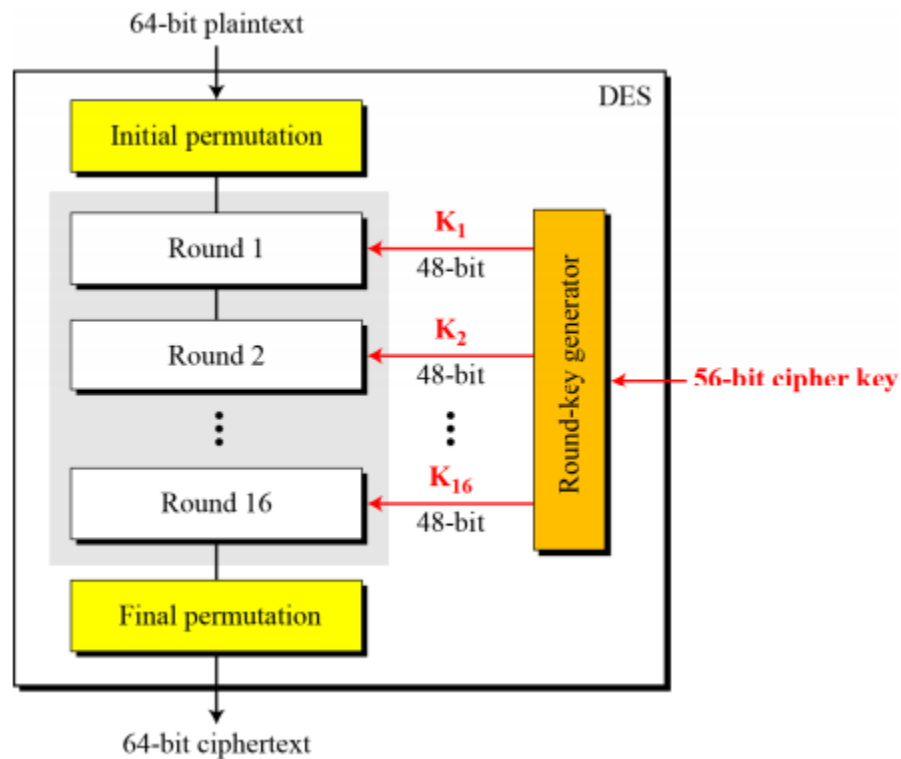
Initial Permutation								*Final Permutation*							
58	50	42	34	26	18	10	02	40	08	48	16	56	24	64	32
60	52	44	36	28	20	12	04	39	07	47	15	55	23	63	31
62	54	46	38	30	22	14	06	38	06	46	14	54	22	62	30
64	56	48	40	32	24	16	08	37	05	45	13	53	21	61	29
57	49	41	33	25	17	09	01	36	04	44	12	52	20	60	28
59	51	43	35	27	19	11	03	35	03	43	11	51	19	59	27
61	53	45	37	29	21	13	05	34	02	42	10	50	18	58	26
63	55	47	39	31	23	15	07	33	01	41	09	49	17	57	25
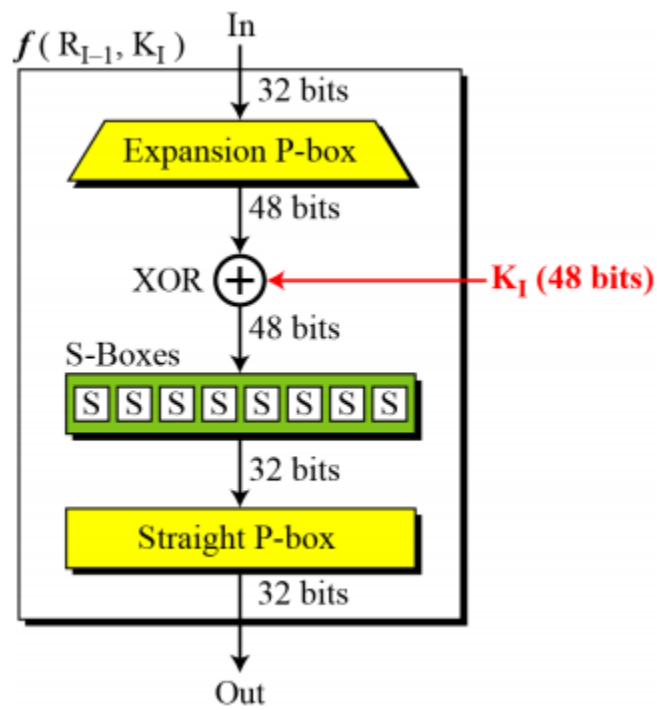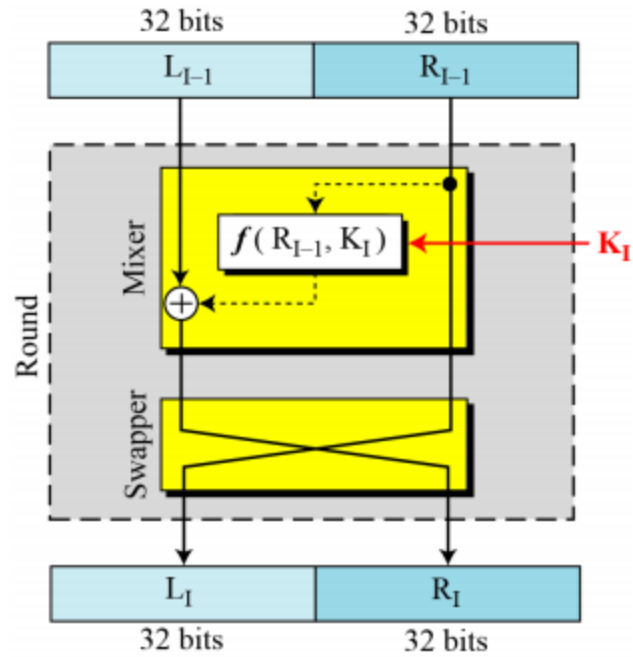
32 bits   32 bits

L_{I-1} R_{I-1}

Round

Mixer

$f(R_{I-1}, K_I)$

K_I

Swapper

L_I R_I

32 bits   32 bits

$f(R_{I-1}, K_I)$

In

32 bits

Expansion P-box

48 bits

XOR K_I (48 bits)

48 bits

S-Boxes

S S S S S S S S

32 bits

Straight P-box

32 bits

Out

	x0000x	x0001x	x0010x	x0011x	x0100x	x0101x	x0110x	x0111x	x1000x	x1001x	x1010x	x1011x	x1100x	x1101x	x1110x	x1111x
0yyyy0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
0yyyy1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
1yyyy0	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
1yyyy1	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

S-box 1

	x0000x	x0001x	x0010x	x0011x	x0100x	x0101x	x0110x	x0111x	x1000x	x1001x	x1010x	x1011x	x1100x	x1101x	x1110x	x1111x
0yyyy0	15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
0yyyy1	3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
1yyyy0	0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
1yyyy1	13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9

S-box 2

	x0000x	x0001x	x0010x	x0011x	x0100x	x0101x	x0110x	x0111x	x1000x	x1001x	x1010x	x1011x	x1100x	x1101x	x1110x	x1111x
0yyyy0	10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
0yyyy1	13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
1yyyy0	13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
1yyyy1	1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12

S-box 3

	x0000x	x0001x	x0010x	x0011x	x0100x	x0101x	x0110x	x0111x	x1000x	x1001x	x1010x	x1011x	x1100x	x1101x	x1110x	x1111x
0yyyy0	7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
0yyyy1	13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
1yyyy0	10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
1yyyy1	3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14

S-box 4

	x0000x	x0001x	x0010x	x0011x	x0100x	x0101x	x0110x	x0111x	x1000x	x1001x	x1010x	x1011x	x1100x	x1101x	x1110x	x1111x
0yyyy0	2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
0yyyy1	14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
1yyyy0	4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
1yyyy1	11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3

S-box 5

	x0000x	x0001x	x0010x	x0011x	x0100x	x0101x	x0110x	x0111x	x1000x	x1001x	x1010x	x1011x	x1100x	x1101x	x1110x	x1111x
0yyyy0	12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
0yyyy1	10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
1yyyy0	9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
1yyyy1	4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13

S-box 6

	x0000x	x0001x	x0010x	x0011x	x0100x	x0101x	x0110x	x0111x	x1000x	x1001x	x1010x	x1011x	x1100x	x1101x	x1110x	x1111x
0yyyy0	4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
0yyyy1	13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
1yyyy0	1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
1yyyy1	6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12

S-box 7

	x0000x	x0001x	x0010x	x0011x	x0100x	x0101x	x0110x	x0111x	x1000x	x1001x	x1010x	x1011x	x1100x	x1101x	x1110x	x1111x
0yyyy0	13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
0yyyy1	1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
1yyyy0	7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
1yyyy1	2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

S-box 8

Straight Pbox:

16	07	20	21	29	12	28	17
01	15	23	26	05	18	31	10
02	08	24	14	32	27	03	09
19	13	30	06	22	11	04	25

Shifting

Rounds	Shift
1, 2, 9, 16	one bit
Others	two bits
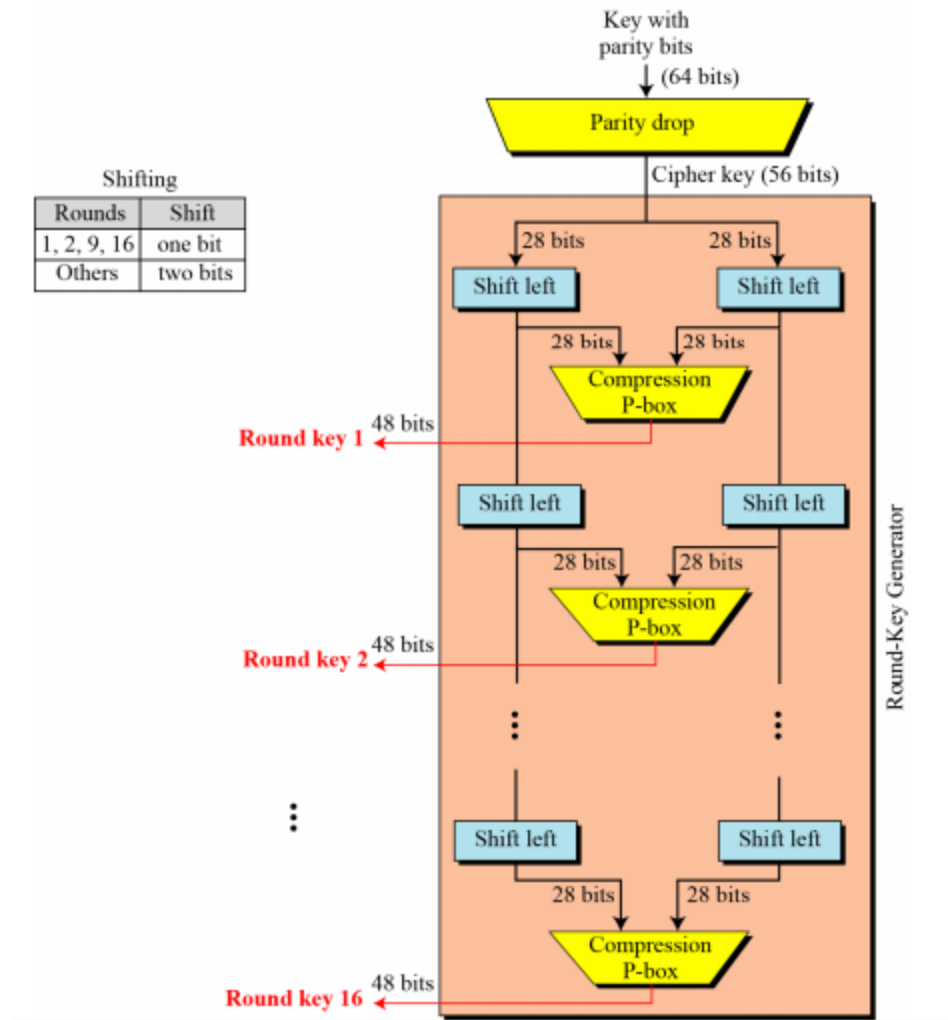
PC-1:

57	49	41	33	25	17	09	01
58	50	42	34	26	18	10	02
59	51	43	35	27	19	11	03
60	52	44	36	63	55	47	39
31	23	15	07	62	54	46	38
30	22	14	06	61	53	45	37
29	21	13	05	28	20	12	04

PC-2:

14	17	11	24	01	05	03	28
15	06	21	10	23	19	12	04
26	08	16	07	27	20	13	02
41	52	31	37	47	55	30	40
51	45	33	48	44	49	39	56
34	53	46	42	50	36	29	32

AES

Nr	Key size
10	128
12	192
14	256

Relationship between number of rounds and cipher key size

State

Round

SubBytes

State

ShiftRows

State

MixColumns

State

AddRoundKey ← **Round key**

State

Notes:

1. One AddRoundKey is applied before the first round.

2. The third transformation is missing in the last round.
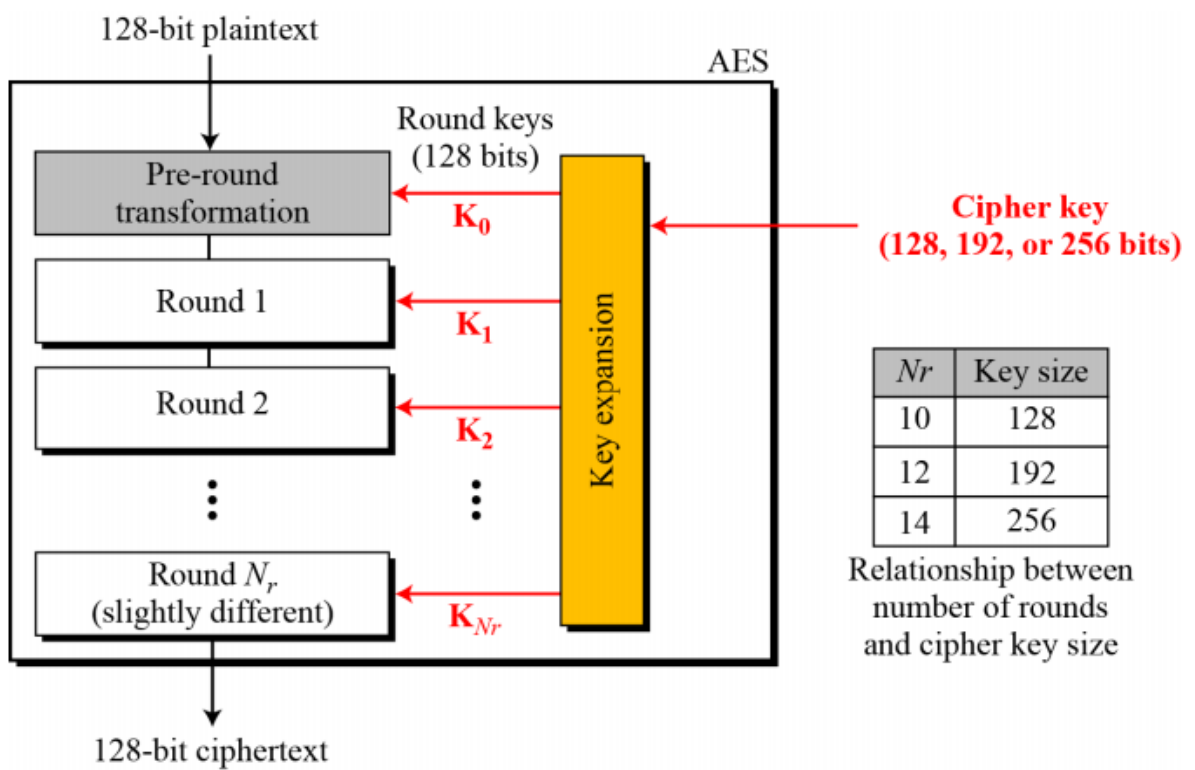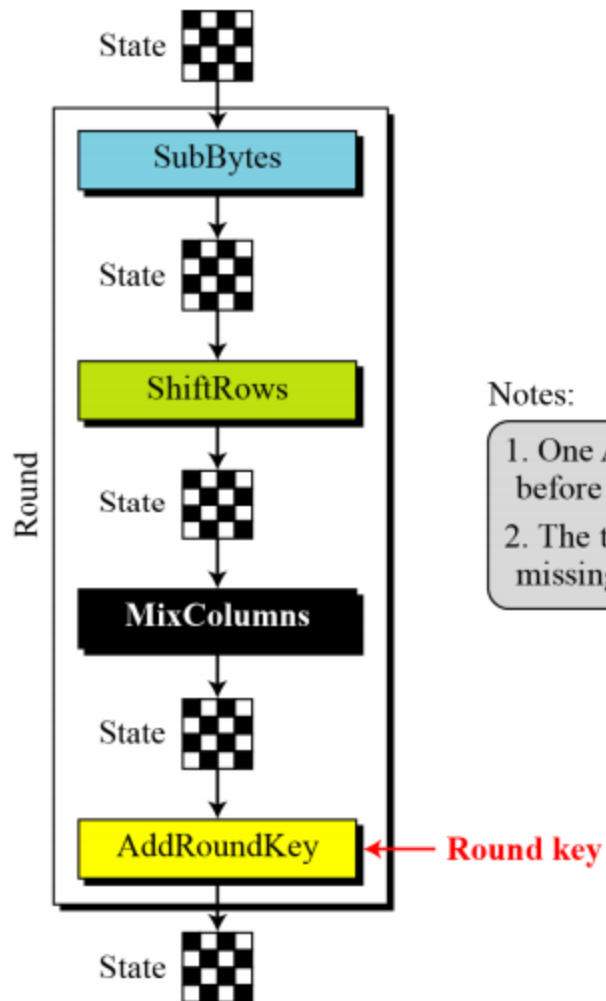
SubBytes Table:

	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	CB	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

InvSubBytes Table:

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
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

Constant matrix in MixColumn:

$$
\begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix}
\xleftrightarrow{\text{Inverse}}
\begin{bmatrix} 0E & 0B & 0D & 09 \\ 09 & 0E & 0B & 0D \\ 0D & 09 & 0E & 0B \\ 0B & 0D & 09 & 0E \end{bmatrix}
$$

$$C \qquad\qquad C^{-1}$$

Rcon:

Round	Constant (RCon)	Round	Constant (RCon)
1	$(\underline{01}\ 00\ 00\ 00)_{16}$	6	$(\underline{20}\ 00\ 00\ 00)_{16}$
2	$(\underline{02}\ 00\ 00\ 00)_{16}$	7	$(\underline{40}\ 00\ 00\ 00)_{16}$
3	$(\underline{04}\ 00\ 00\ 00)_{16}$	8	$(\underline{80}\ 00\ 00\ 00)_{16}$
4	$(\underline{08}\ 00\ 00\ 00)_{16}$	9	$(\underline{1B}\ 00\ 00\ 00)_{16}$
5	$(\underline{10}\ 00\ 00\ 00)_{16}$	10	$(\underline{36}\ 00\ 00\ 00)_{16}$

Key Generating:

Making of t_i (temporary) words $i = 4\ N_r$
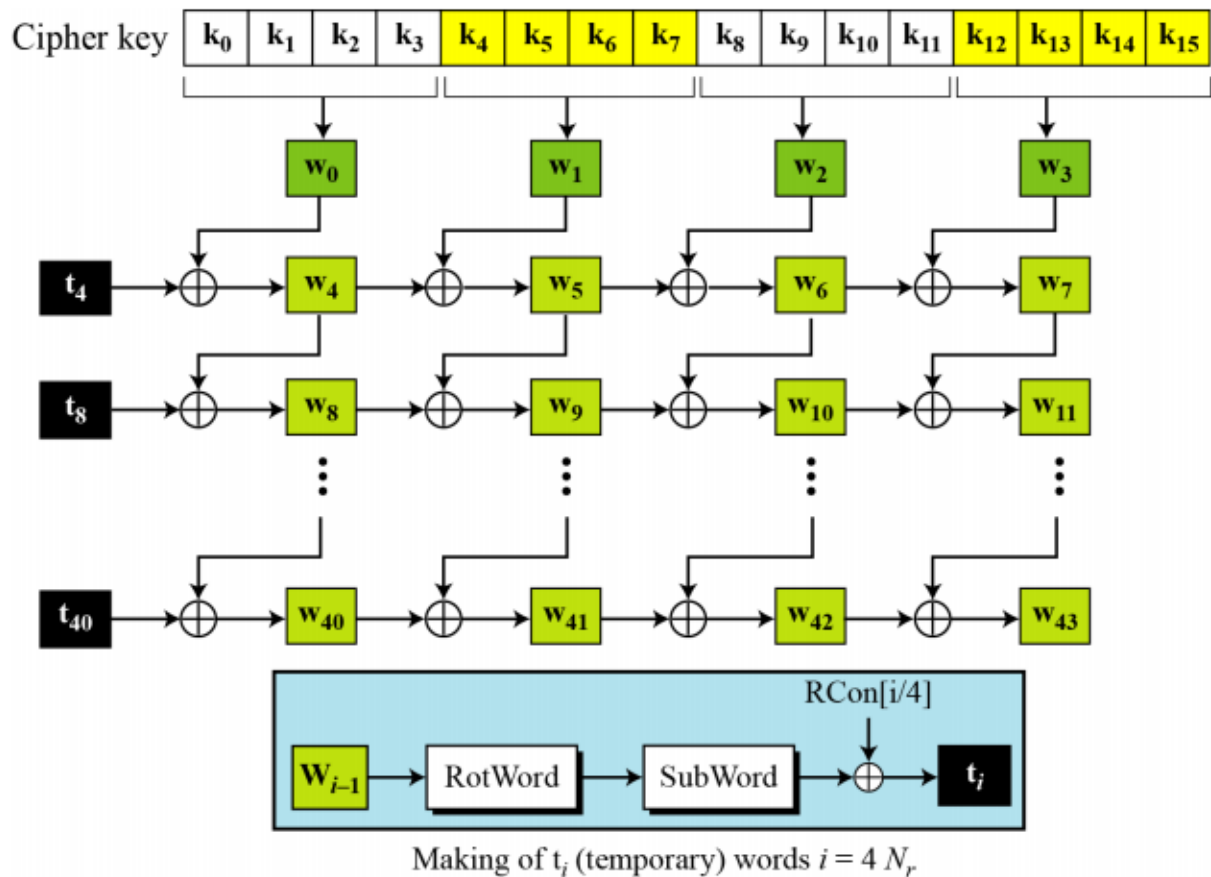
RSA

4. Encryption and Decryption

❖ *RSA Decryption*

- *Example (cont.)* Decryption using Private Key: $P = 401^{581} \pmod{1541} = 66$.
  - Using method of Square and Multiply. Power: $d = 581 = (1001000101)_2$. Initialization: $P_1 = 1$.

bit	P_1	$P_1 = P_1^2 \bmod 1541$	$P_1 = (P_1 \cdot 401) \bmod 1541$ if bit '1'. $P_1 = P_1$ if bit '0'
1	1	$1^2 \bmod 1541 = 1$	$(1 \cdot 401) \bmod 1541 = 401$
0	401	$401^2 \bmod 1541 = 537$	537
0	537	$537^2 \bmod 1541 = 202$	202
1	202	$202^2 \bmod 1541 = 738$	$(738 \cdot 401) \bmod 1541 = 66$
0	66	$66^2 \bmod 1541 = 1274$	1274
0	1274	$1274^2 \bmod 1541 = 403$	403
0	403	$403^2 \bmod 1541 = 604$	604
1	604	$604^2 \bmod 1541 = 1140$	$(1140 \cdot 401) \bmod 1541 = 1004$
0	1004	$1004^2 \bmod 1541 = 202$	202
1	202	$202^2 \bmod 1541 = 738$	$(738 \cdot 401) \bmod 1541 = 66 = P$

SHA

Results of the previous block or the initial digest

Round 0

Round 79

W_0

K_0

W_{79}

K_{79}

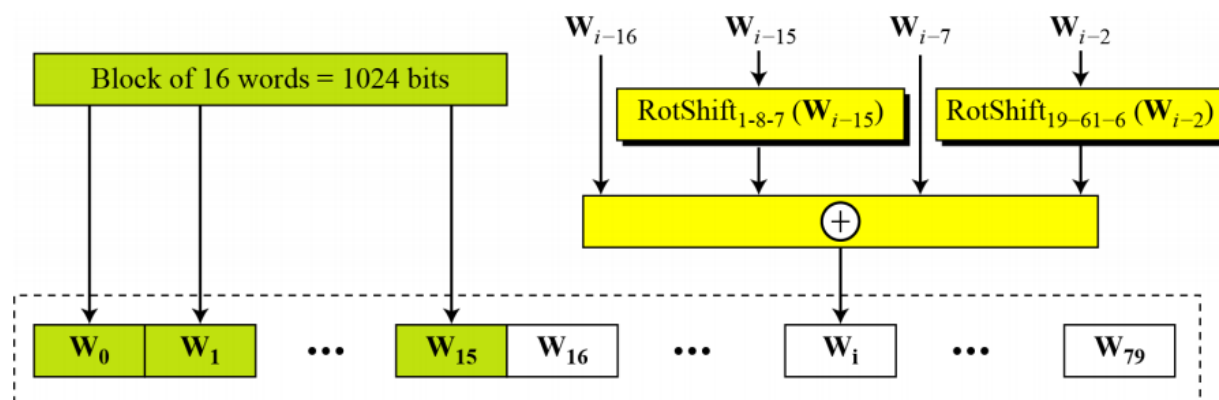Final adding

Values for the next block or the final digest
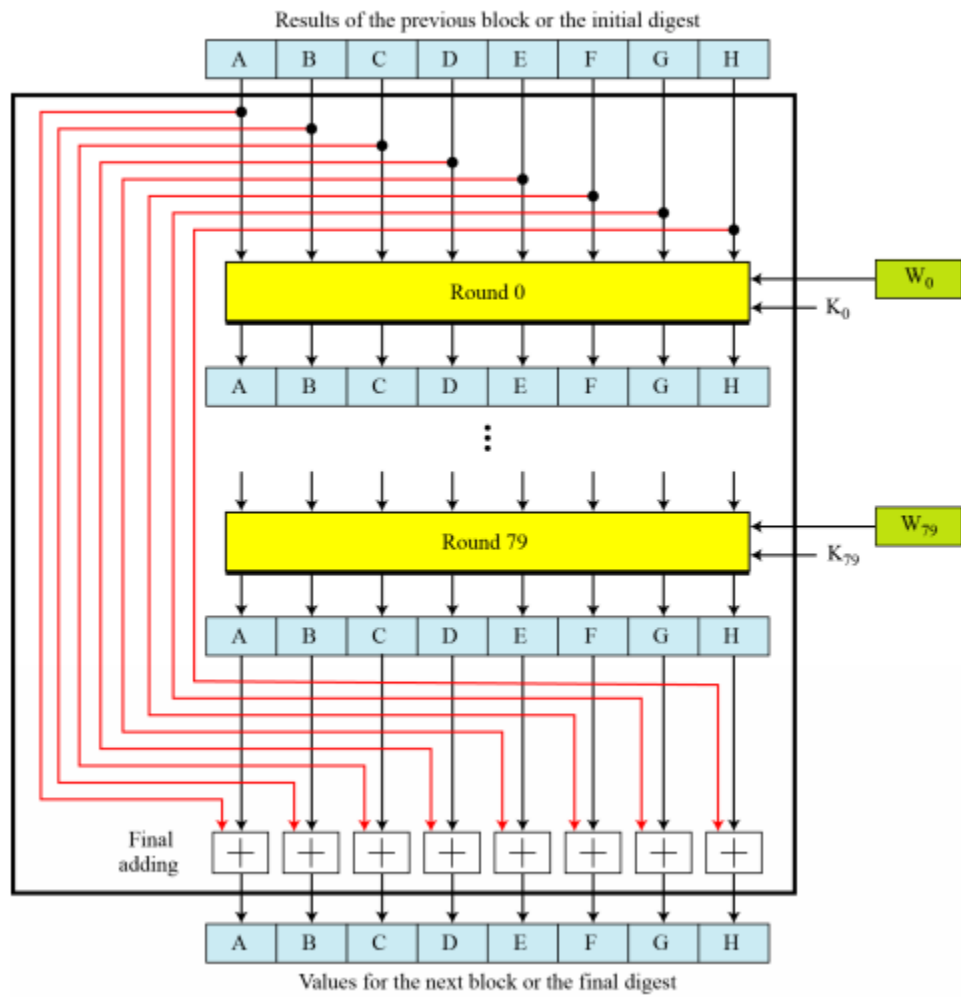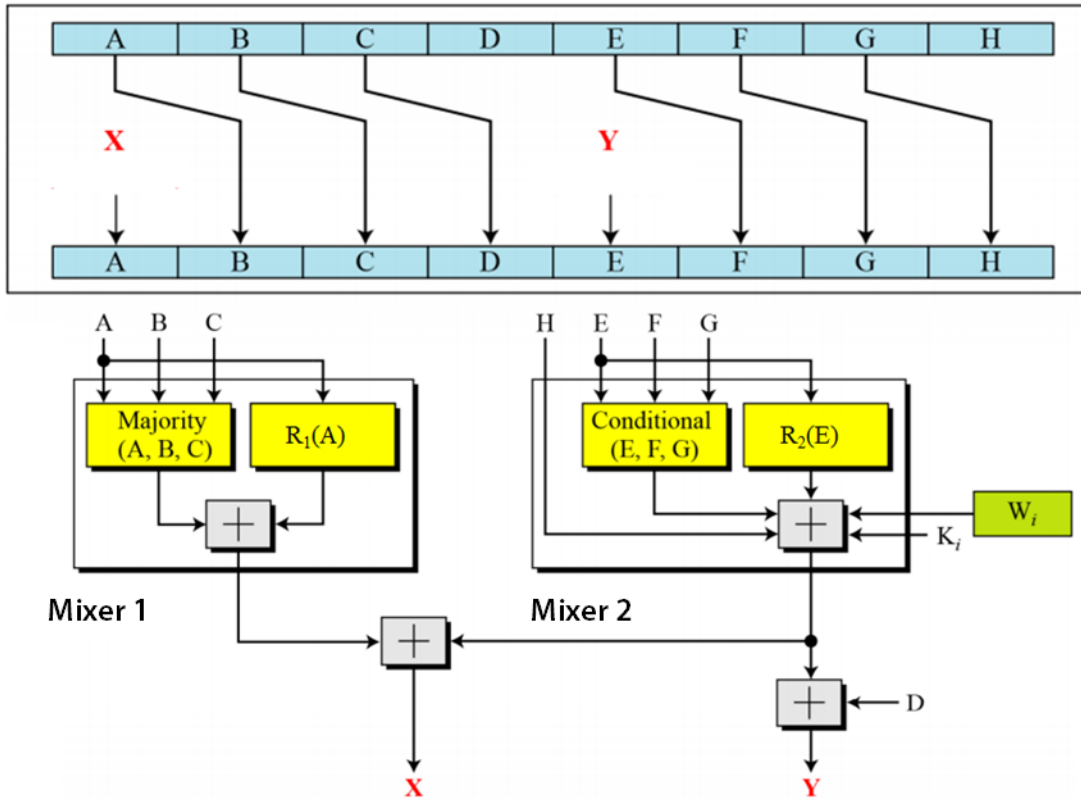
$$\text{Majority}(x, y, z) = (x \,\&\, y) \oplus (y \,\&\, z) \oplus (z \,\&\, x)$$

$$\text{Conditional}(x, y, z) = (x \,\&\, y) \oplus (\sim x \,\&\, z)$$

$$R_1(x) = \text{RotR}(x, 28) \oplus \text{RotR}(x, 34) \oplus \text{RotR}(x, 39)$$

$$R_2(x) = \text{RotR}(x, 14) \oplus \text{RotR}(x, 18) \oplus \text{RotR}(x, 41)$$

Word Expansion

$$\text{RotShift}_{l\text{-}m\text{-}n}(x): \text{RotR}_l(x) \oplus \text{RotR}_m(x) \oplus \text{ShR}_n(x)$$

$\text{RotR}_i(x)$: Right-rotation of the argument x by i bits

$\text{ShR}_i(x)$: Shift-left of the argument x by i bits and padding the left by 0's.

I = 0 ÷ 19	I = 20 ÷ 39	I = 40 ÷ 59	I = 60 ÷ 79
428A2F98D728AE22	2DE92C6F592B0275	A2BFE8A14CF10364	90BEFFFA23631E28
7137449123EF65CD	4A7484AA6EA6E483	A81A664BBC423001	A4506CEBDE82BDE9
B5C0FBCFEC4D3B2F	5CB0A9DCBD41FBD4	C24B8B70D0F89791	BEF9A3F7B2C67915
E9B5DBA58189DBBC	76F988DA831153B5	C76C51A30654BE30	C67178F2E372532B
3956C25BF348B538	983E5152EE66DFAB	D192E819D6EF5218	CA273ECEEA26619C
59F111F1B605D019	A831C66D2DB43210	D69906245565A910	D186B8C721C0C207
923F82A4AF194F9B	B00327C898FB213F	F40E35855771202A	EADA7DD6CDE0EB1E
AB1C5ED5DA6D8118	BF597FC7BEEF0EE4	106AA07032BBD1B8	F57D4F7FEE6ED178
D807AA98A3030242	C6E00BF33DA88FC2	19A4C116B8D2D0C8	06F067AA72176FBA
12835B0145706FBE	D5A79147930AA725	1E376C085141AB53	0A637DC5A2C898A6
243185BE4EE4B28C	06CA6351E003826F	2748774CDF8EEB99	113F9804BEF90DAE
550C7DC3D5FFB4E2	142929670A0E6E70	34B0BCB5E19B48A8	1B710B35131C471B
72BE5D74F27B896F	27B70A8546D22FFC	391C0CB3C5C95A63	28DB77F523047D84
80DEB1FE3B1696B1	2E1B21385C26C926	4ED8AA4AE3418ACB	32CAAB7B40C72493
9BDC06A725C71235	4D2C6DFC5AC42AED	5B9CCA4F7763E373	3C9EBE0A15C9BEBC
C19BF174CF692694	53380D139D95B3DF	682E6FF3D6B2B8A3	431D67C49C100D4C
E49B69C19EF14AD2	650A73548BAF63DE	748F82EE5DEFB2FC	4CC5D4BECB3E42B6
EFBE4786384F25E3	766A0ABB3C77B2A8	78A5636F43172F60	597F299CFC657E2A
0FC19DC68B8CD5B5	81C2C92E47EDAEE6	84C87814A1F0AB72	5FCB6FAB3AD6FAEC
240CA1CC77AC9C65	92722C851482353B	8CC702081A6439EC	6C44198C4A475817