DES (Data Encryption Standard)

1 Core functions

Algorithm 1 DES cipher

1: **function** CIPHER($block$, $subkeys$)
2: $block$ = IP($block$) ▷ initial permutation (IP)
3: split into $left$ and $right$ halves
4: **for** 16 rounds, **do**
5: $left_{i+1} = right_i$
6: $right_{i+1} = left_i \oplus$ Feistel($right_i, subkey[i]$) ▷ Feistel (F) function
7: $block$ = concatenate halves
8: $block = \text{IP}^{-1}(block)$ ▷ final permutation (IP^{-1})
9: **return** $block$

Algorithm 2 Feistel (F) function

1: **function** FEISTEL($block$, $subkey$)
2: $block$ = expansion($block$) ▷ expansion permutation (E)
3: $block = block \oplus subkey$
4: $block$ = s-boxes($block$) ▷ substitution boxes (s-boxes)
5: $block$ = p-box($block$) ▷ p-box permutation (P)
6: **return** $block$

Algorithm 3 Key schedule

1: **function** KEY SCHEDULE(key)
2: key = PC-1(key) ▷ permuted choice 1 (PC-1)
3: split into $left$ and $right$ halves
4: **for** 16 rounds, **do**
5: $left$ = left rotate($left, rotation[i]$) ▷ rotation table
6: $right$ = left rotate($right, rotation[i]$)
7: $block$ = concatenate halves
8: $subkey[i]$ = PC-2($block$) ▷ permuted choice 2 (PC-2)
9: **return** $subkeys$

2 Substitution boxes (s-boxes)

The 48-bit block is divided into 8 pieces of 6-bits each. Each 6-bit input is replaced with 4-bit output, according to the lookup table.

- the **nth of the sextet** refers to the **box**
- the first and last bit of the sextet are combined into a **2-bit value** which refers to the **row**
- the inner 4 bits of the sextet become a **4-bit value** which refers to the **column**

Algorithm 4 substitution boxes (s-boxes)

```
1: function S-BOXES(input)
2:     for 8 rounds, do
3:         sextet = input[i]                          ▷ input clumped by 6 bits
4:         outer = first and last bit of sextet
5:         inner = middle 4 bits of sextet
6:         quartet = table[i][outer][inner]           ▷ s-box lookup table
7:         output[i] = quartet                        ▷ output clumped by 4 bits
8:     return output
```

2.1 Box 0

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	0xE	0x4	0xD	0x1	0x2	0xF	0xB	0x8	0x3	0xA	0x6	0xC	0x5	0x9	0x0	0x7
1	0x0	0xF	0x7	0x4	0xE	0x2	0xD	0x1	0xA	0x6	0xC	0xB	0x9	0x5	0x3	0x8
2	0x4	0x1	0xE	0x8	0xD	0x6	0x2	0xB	0xF	0xC	0x9	0x7	0x3	0xA	0x5	0x0
3	0xF	0xC	0x8	0x2	0x4	0x9	0x1	0x7	0x5	0xB	0x3	0xE	0xA	0x0	0x6	0xD

2.2 Box 1

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	0xF	0x1	0x8	0xE	0x6	0xB	0x3	0x4	0x9	0x7	0x2	0xD	0xC	0x0	0x5	0xA
1	0x3	0xD	0x4	0x7	0xF	0x2	0x8	0xE	0xC	0x0	0x1	0xA	0x6	0x9	0xB	0x5
2	0x0	0xE	0x7	0xB	0xA	0x4	0xD	0x1	0x5	0x8	0xC	0x6	0x9	0x3	0x2	0xF
3	0xD	0x8	0xA	0x1	0x3	0xF	0x4	0x2	0xB	0x6	0x7	0xC	0x0	0x5	0xE	0x9

2.3 Box 2

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	0xA	0x0	0x9	0xE	0x6	0x3	0xF	0x5	0x1	0xD	0xC	0x7	0xB	0x4	0x2	0x8
1	0xD	0x7	0x0	0x9	0x3	0x4	0x6	0xA	0x2	0x8	0x5	0xE	0xC	0xB	0xF	0x1
2	0xD	0x6	0x4	0x9	0x8	0xF	0x3	0x0	0xB	0x1	0x2	0xC	0x5	0xA	0xE	0x7
3	0x1	0xA	0xD	0x0	0x6	0x9	0x8	0x7	0x4	0xF	0xE	0x3	0xB	0x5	0x2	0xC

2.4 Box 3

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	0x7	0xD	0xE	0x3	0x0	0x6	0x9	0xA	0x1	0x2	0x8	0x5	0xB	0xC	0x4	0xF
1	0xD	0x8	0xB	0x5	0x6	0xF	0x0	0x3	0x4	0x7	0x2	0xC	0x1	0xA	0xE	0x9
2	0xA	0x6	0x9	0x0	0xC	0xB	0x7	0xD	0xF	0x1	0x3	0xE	0x5	0x2	0x8	0x4
3	0x3	0xF	0x0	0x6	0xA	0x1	0xD	0x8	0x9	0x4	0x5	0xB	0xC	0x7	0x2	0xE

2.5 Box 4

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	0x2	0xC	0x4	0x1	0x7	0xA	0xB	0x6	0x8	0x5	0x3	0xF	0xD	0x0	0xE	0x9
1	0xE	0xB	0x2	0xC	0x4	0x7	0xD	0x1	0x5	0x0	0xF	0xA	0x3	0x9	0x8	0x6
2	0x4	0x2	0x1	0xB	0xA	0xD	0x7	0x8	0xF	0x9	0xC	0x5	0x6	0x3	0x0	0xE
3	0xB	0x8	0xC	0x7	0x1	0xE	0x2	0xD	0x6	0xF	0x0	0x9	0xA	0x4	0x5	0x3

2.6 Box 5

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	0xC	0x1	0xA	0xF	0x9	0x2	0x6	0x8	0x0	0xD	0x3	0x4	0xE	0x7	0x5	0xB
1	0xA	0xF	0x4	0x2	0x7	0xC	0x9	0x5	0x6	0x1	0xD	0xE	0x0	0xB	0x3	0x8
2	0x9	0xE	0xF	0x5	0x2	0x8	0xC	0x3	0x7	0x0	0x4	0xA	0x1	0xD	0xB	0x6
3	0x4	0x3	0x2	0xC	0x9	0x5	0xF	0xA	0xB	0xE	0x1	0x7	0x6	0x0	0x8	0xD

2.7 Box 6

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	0x4	0xB	0x2	0xE	0xF	0x0	0x8	0xD	0x3	0xC	0x9	0x7	0x5	0xA	0x6	0x1
1	0xD	0x0	0xB	0x7	0x4	0x9	0x1	0xA	0xE	0x3	0x5	0xC	0x2	0xF	0x8	0x6
2	0x1	0x4	0xB	0xD	0xC	0x3	0x7	0xE	0xA	0xF	0x6	0x8	0x0	0x5	0x9	0x2
3	0x6	0xB	0xD	0x8	0x1	0x4	0xA	0x7	0x9	0x5	0x0	0xF	0xE	0x2	0x3	0xC

2.8 Box 7

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	0xD	0x2	0x8	0x4	0x6	0xF	0xB	0x1	0xA	0x9	0x3	0xE	0x5	0x0	0xC	0x7
1	0x1	0xF	0xD	0x8	0xA	0x3	0x7	0x4	0xC	0x5	0x6	0xB	0x0	0xE	0x9	0x2
2	0x7	0xB	0x4	0x1	0x9	0xC	0xE	0x2	0x0	0x6	0xA	0xD	0xF	0x3	0x5	0x8
3	0x2	0x1	0xE	0x7	0x4	0xA	0x8	0xD	0xF	0xC	0x9	0x0	0x3	0x5	0x6	0xB