FORMALIZED MATHEMATICS
Vol. 20, No. 2, Pages 125–146, 2012
DOI: 10.2478/v10037-012-0016-y

VERSITA
versita.com/fm/

Formalization of the Data Encryption Standard[1]

Hiroyuki Okazaki
Shinshu University
Nagano, Japan

Yasunari Shidama
Shinshu University
Nagano, Japan

Summary. In this article we formalize DES (the Data Encryption Standard), that was the most widely used symmetric cryptosystem in the world. DES is a block cipher which was selected by the National Bureau of Standards as an official Federal Information Processing Standard for the United States in 1976 [15].

MML identifier: DESCIP_1, version: 7.12.02 4.181.1147

The papers [14], [5], [12], [1], [16], [4], [6], [18], [11], [7], [8], [17], [20], [2], [3], [9], [21], [22], [13], [19], and [10] provide the terminology and notation for this paper.

1. Preliminaries

Let n be a natural number and let f be an n-element finite sequence. Note that $\mathrm{Rev}(f)$ is n-element.

Let D be a non empty set, let n be a natural number, and let f be an element of D^n. Then $\mathrm{Rev}(f)$ is an element of D^n.

Let n be a natural number and let f be a finite sequence. We introduce Op-Left(f, n) as a synonym of $f{\restriction}n$. We introduce Op-Right(f, n) as a synonym of $f_{\lfloor n}$.

Let D be a non empty set, let n be a natural number, and let f be a finite sequence of elements of D. Then Op-Left(f, n) is a finite sequence of elements of D. Then Op-Right(f, n) is a finite sequence of elements of D.

[1]This work was supported by JSPS KAKENHI 21240001.

ISSN 1426–2630(p), 1898-9934(e)

Let D be a non empty set, let n be a natural number, and let s be an element of $D^{2 \cdot n}$. We introduce SP-Left s as a synonym of Op-Left(s, n). We introduce SP-Right s as a synonym of Op-Right(s, n).

Let D be a non empty set, let n be a natural number, and let s be an element of $D^{2 \cdot n}$. Then SP-Left s is an element of D^n.

One can prove the following propositions:

(1) For all non empty elements m, n of $\mathbb{N}$ and for every element s of D^n such that $m \leq n$ holds Op-Left(s, m) is an element of D^m.

(2) Let m, n, l be non empty elements of $\mathbb{N}$ and s be an element of D^n. If $m \leq n$ and $l = n - m$, then Op-Right(s, m) is an element of D^l.

Let D be a non empty set, let n be a non empty element of $\mathbb{N}$, and let s be an element of $D^{2 \cdot n}$. Then SP-Right s is an element of D^n.

Next we state the proposition

(3) For every non empty element n of $\mathbb{N}$ and for every element s of $D^{2 \cdot n}$ holds (SP-Left s) $\frown$ SP-Right $s = s$.

Let s be a finite sequence. The functor Op-LeftShift s yielding a finite sequence is defined by:

(Def. 1) Op-LeftShift $s = (s_{\lfloor 1}) \frown \langle s(1) \rangle$.

Next we state three propositions:

(4) For every finite sequence s such that $1 \leq \operatorname{len} s$ holds len Op-LeftShift $s = \operatorname{len} s$.

(5) If $1 \leq \operatorname{len} s$, then Op-LeftShift s is a finite sequence of elements of D and len Op-LeftShift $s = \operatorname{len} s$.

(6) For every non empty element n of $\mathbb{N}$ and for every element s of D^n holds Op-LeftShift s is an element of D^n.

Let s be a finite sequence. The functor Op-RightShift s yields a finite sequence and is defined by:

(Def. 2) Op-RightShift $s = (\langle s(\operatorname{len} s) \rangle \frown s) \restriction \operatorname{len} s$.

One can prove the following three propositions:

(7) For every finite sequence s holds len Op-RightShift $s = \operatorname{len} s$.

(8) If $1 \leq \operatorname{len} s$, then Op-RightShift s is a finite sequence of elements of D and len Op-RightShift $s = \operatorname{len} s$.

(9) For every non empty element n of $\mathbb{N}$ and for every element s of D^n holds Op-RightShift s is an element of D^n.

Let D be a non empty set, let s be a finite sequence of elements of D, and let n be an integer. Let us assume that $1 \leq \operatorname{len} s$. The functor Op-Shift$(s, n)$ yields a finite sequence of elements of D and is defined by:

(Def. 3) len Op-Shift$(s, n) = \operatorname{len} s$ and for every natural number i such that $i \in \operatorname{Seg} \operatorname{len} s$ holds $(\text{Op-Shift}(s, n))(i) = s((((i - 1) + n) \bmod \operatorname{len} s) + 1)$.

The following propositions are true:

(10) For all integers n, m such that $1 \leq \operatorname{len} s$ holds $\text{Op-Shift}(\text{Op-Shift}(s, n), m) = \text{Op-Shift}(s, n + m)$.

(11) If $1 \leq \operatorname{len} s$, then $\text{Op-Shift}(s, 0) = s$.

(12) If $1 \leq \operatorname{len} s$, then $\text{Op-Shift}(s, \operatorname{len} s) = s$.

(13) If $1 \leq \operatorname{len} s$, then $\text{Op-Shift}(s, -\operatorname{len} s) = s$.

(14) Let n be a non empty element of $\mathbb{N}$, m be an integer, and s be an element of D^n. Then $\text{Op-Shift}(s, m)$ is an element of D^n.

(15) If $1 \leq \operatorname{len} s$, then $\text{Op-Shift}(s, -1) = \text{Op-RightShift}\, s$.

(16) If $1 \leq \operatorname{len} s$, then $\text{Op-Shift}(s, 1) = \text{Op-LeftShift}\, s$.

Let x, y be elements of $\mathit{Boolean}^{28}$. Then $x \frown y$ is an element of $\mathit{Boolean}^{56}$.

Let n be a non empty element of $\mathbb{N}$, let s be an element of $\mathit{Boolean}^n$, and let i be a natural number. Then $s(i)$ is an element of *Boolean*.

Let n be a non empty element of $\mathbb{N}$, let s be an element of $\mathbb{N}^n$, and let i be a natural number. Then $s(i)$ is an element of $\mathbb{N}$.

Let n be a natural number. Observe that every element of $\mathit{Boolean}^n$ is boolean-valued.

Let n be an element of $\mathbb{N}$ and let s, t be elements of $\mathit{Boolean}^n$. We introduce $\text{Op-XOR}(s, t)$ as a synonym of $s \oplus t$.

Let n be a non empty element of $\mathbb{N}$ and let s, t be elements of $\mathit{Boolean}^n$. Then $\text{Op-XOR}(s, t)$ is an element of $\mathit{Boolean}^n$ and it can be characterized by the condition:

(Def. 4) For every natural number i such that $i \in \operatorname{Seg} n$ holds $(\text{Op-XOR}(s, t))(i) = s(i) \oplus t(i)$.

Let us notice that the functor $\text{Op-XOR}(s, t)$ is commutative.

Let n, k be non empty elements of $\mathbb{N}$, let R_1 be an element of $(\mathit{Boolean}^n)^k$, and let i be an element of $\operatorname{Seg} k$. Then $R_1(i)$ is an element of $\mathit{Boolean}^n$.

We now state the proposition

(17) For every non empty element n of $\mathbb{N}$ and for all elements s, t of $\mathit{Boolean}^n$ holds $\text{Op-XOR}(\text{Op-XOR}(s, t), t) = s$.

Let m be a non empty element of $\mathbb{N}$, let D be a non empty set, let L be a sequence of D^m, and let i be a natural number. Then $L(i)$ is an element of D^m.

Let f be a function from 64 into 16 and let i be a set. Then $f(i)$ is an element of 16.

Next we state the proposition

(18) For all natural numbers n, m such that $n + m \leq \operatorname{len} s$ holds $(s \restriction n) \frown (s_{\lfloor n} \restriction m) = s \restriction (n + m)$.

The scheme *QuadChoiceRec* deals with non empty sets $\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{D}$, an element $\mathcal{E}$ of $\mathcal{A}$, an element $\mathcal{F}$ of $\mathcal{B}$, an element $\mathcal{G}$ of $\mathcal{C}$, an element $\mathcal{H}$ of $\mathcal{D}$, and a 9-ary predicate $\mathcal{P}$, and states that:

There exists a function f from $\mathbb{N}$ into $\mathcal{A}$ and there exists a function g from $\mathbb{N}$ into $\mathcal{B}$ and there exists a function h from $\mathbb{N}$ into $\mathcal{C}$ and there exists a function i from $\mathbb{N}$ into $\mathcal{D}$ such that $f(0) = \mathcal{E}$ and $g(0) = \mathcal{F}$ and $h(0) = \mathcal{G}$ and $i(0) = \mathcal{H}$ and for every element n of $\mathbb{N}$ holds $\mathcal{P}[n, f(n), g(n), h(n), i(n), f(n+1), g(n+1), h(n+1), i(n+1)]$

provided the following condition is satisfied:

- Let n be an element of $\mathbb{N}$, x be an element of $\mathcal{A}$, y be an element of $\mathcal{B}$, z be an element of $\mathcal{C}$, and w be an element of $\mathcal{D}$. Then there exists an element x_1 of $\mathcal{A}$ and there exists an element y_1 of $\mathcal{B}$ and there exists an element z_1 of $\mathcal{C}$ and there exists an element w_1 of $\mathcal{D}$ such that $\mathcal{P}[n, x, y, z, w, x_1, y_1, z_1, w_1]$.

Next we state a number of propositions:

(19) Let x be a set. Suppose $x \in \operatorname{Seg} 16$. Then $x = 1$ or $x = 2$ or $x = 3$ or $x = 4$ or $x = 5$ or $x = 6$ or $x = 7$ or $x = 8$ or $x = 9$ or $x = 10$ or $x = 11$ or $x = 12$ or $x = 13$ or $x = 14$ or $x = 15$ or $x = 16$.

(20) Let x be a set. Suppose $x \in \operatorname{Seg} 32$. Then $x = 1$ or $x = 2$ or $x = 3$ or $x = 4$ or $x = 5$ or $x = 6$ or $x = 7$ or $x = 8$ or $x = 9$ or $x = 10$ or $x = 11$ or $x = 12$ or $x = 13$ or $x = 14$ or $x = 15$ or $x = 16$ or $x = 17$ or $x = 18$ or $x = 19$ or $x = 20$ or $x = 21$ or $x = 22$ or $x = 23$ or $x = 24$ or $x = 25$ or $x = 26$ or $x = 27$ or $x = 28$ or $x = 29$ or $x = 30$ or $x = 31$ or $x = 32$.

(21) Let x be a set. Suppose $x \in \operatorname{Seg} 48$. Then $x = 1$ or $x = 2$ or $x = 3$ or $x = 4$ or $x = 5$ or $x = 6$ or $x = 7$ or $x = 8$ or $x = 9$ or $x = 10$ or $x = 11$ or $x = 12$ or $x = 13$ or $x = 14$ or $x = 15$ or $x = 16$ or $x = 17$ or $x = 18$ or $x = 19$ or $x = 20$ or $x = 21$ or $x = 22$ or $x = 23$ or $x = 24$ or $x = 25$ or $x = 26$ or $x = 27$ or $x = 28$ or $x = 29$ or $x = 30$ or $x = 31$ or $x = 32$ or $x = 33$ or $x = 34$ or $x = 35$ or $x = 36$ or $x = 37$ or $x = 38$ or $x = 39$ or $x = 40$ or $x = 41$ or $x = 42$ or $x = 43$ or $x = 44$ or $x = 45$ or $x = 46$ or $x = 47$ or $x = 48$.

(22) Let x be a set. Suppose $x \in \operatorname{Seg} 56$. Then $x = 1$ or $x = 2$ or $x = 3$ or $x = 4$ or $x = 5$ or $x = 6$ or $x = 7$ or $x = 8$ or $x = 9$ or $x = 10$ or $x = 11$ or $x = 12$ or $x = 13$ or $x = 14$ or $x = 15$ or $x = 16$ or $x = 17$ or $x = 18$ or $x = 19$ or $x = 20$ or $x = 21$ or $x = 22$ or $x = 23$ or $x = 24$ or $x = 25$ or $x = 26$ or $x = 27$ or $x = 28$ or $x = 29$ or $x = 30$ or $x = 31$ or $x = 32$ or $x = 33$ or $x = 34$ or $x = 35$ or $x = 36$ or $x = 37$ or $x = 38$ or $x = 39$ or $x = 40$ or $x = 41$ or $x = 42$ or $x = 43$ or $x = 44$ or $x = 45$ or $x = 46$ or $x = 47$ or $x = 48$ or $x = 49$ or $x = 50$ or $x = 51$ or $x = 52$ or $x = 53$ or $x = 54$ or $x = 55$ or $x = 56$.

(23) Let x be a set. Suppose $x \in \operatorname{Seg} 64$. Then $x = 1$ or $x = 2$ or $x = 3$ or $x = 4$ or $x = 5$ or $x = 6$ or $x = 7$ or $x = 8$ or $x = 9$ or $x = 10$ or $x = 11$ or $x = 12$ or $x = 13$ or $x = 14$ or $x = 15$ or $x = 16$ or $x = 17$ or $x = 18$ or $x = 19$ or $x = 20$ or $x = 21$ or $x = 22$ or $x = 23$ or $x = 24$ or $x = 25$ or

$x = 26$ or $x = 27$ or $x = 28$ or $x = 29$ or $x = 30$ or $x = 31$ or $x = 32$ or $x = 33$ or $x = 34$ or $x = 35$ or $x = 36$ or $x = 37$ or $x = 38$ or $x = 39$ or $x = 40$ or $x = 41$ or $x = 42$ or $x = 43$ or $x = 44$ or $x = 45$ or $x = 46$ or $x = 47$ or $x = 48$ or $x = 49$ or $x = 50$ or $x = 51$ or $x = 52$ or $x = 53$ or $x = 54$ or $x = 55$ or $x = 56$ or $x = 57$ or $x = 58$ or $x = 59$ or $x = 60$ or $x = 61$ or $x = 62$ or $x = 63$ or $x = 64$.

(24) For every non empty natural number n holds $n = \{0\} \cup (\mathrm{Seg}\, n \setminus \{n\})$.

(25) For every non empty natural number n and for every set x such that $x \in n$ holds $x = 0$ or $x \in \mathrm{Seg}\, n$ and $x \neq n$.

(26) Let x be a set. Suppose $x \in 16$. Then $x = 0$ or $x = 1$ or $x = 2$ or $x = 3$ or $x = 4$ or $x = 5$ or $x = 6$ or $x = 7$ or $x = 8$ or $x = 9$ or $x = 10$ or $x = 11$ or $x = 12$ or $x = 13$ or $x = 14$ or $x = 15$.

(27) Let x be a set. Suppose $x \in 64$. Then $x = 0$ or $x = 1$ or $x = 2$ or $x = 3$ or $x = 4$ or $x = 5$ or $x = 6$ or $x = 7$ or $x = 8$ or $x = 9$ or $x = 10$ or $x = 11$ or $x = 12$ or $x = 13$ or $x = 14$ or $x = 15$ or $x = 16$ or $x = 17$ or $x = 18$ or $x = 19$ or $x = 20$ or $x = 21$ or $x = 22$ or $x = 23$ or $x = 24$ or $x = 25$ or $x = 26$ or $x = 27$ or $x = 28$ or $x = 29$ or $x = 30$ or $x = 31$ or $x = 32$ or $x = 33$ or $x = 34$ or $x = 35$ or $x = 36$ or $x = 37$ or $x = 38$ or $x = 39$ or $x = 40$ or $x = 41$ or $x = 42$ or $x = 43$ or $x = 44$ or $x = 45$ or $x = 46$ or $x = 47$ or $x = 48$ or $x = 49$ or $x = 50$ or $x = 51$ or $x = 52$ or $x = 53$ or $x = 54$ or $x = 55$ or $x = 56$ or $x = 57$ or $x = 58$ or $x = 59$ or $x = 60$ or $x = 61$ or $x = 62$ or $x = 63$.

(28) Let S be a non empty set and x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8 be elements of S. Then there exists a finite sequence s of elements of S such that s is 8-element and $s(1) = x_1$ and $s(2) = x_2$ and $s(3) = x_3$ and $s(4) = x_4$ and $s(5) = x_5$ and $s(6) = x_6$ and $s(7) = x_7$ and $s(8) = x_8$.

(29) Let S be a non empty set and x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8, x_9, x_{10}, x_{11}, x_{12}, x_{13}, x_{14}, x_{15}, x_{16} be elements of S. Then there exists a finite sequence s of elements of S such that
s is 16-element and $s(1) = x_1$ and $s(2) = x_2$ and $s(3) = x_3$ and $s(4) = x_4$ and $s(5) = x_5$ and $s(6) = x_6$ and $s(7) = x_7$ and $s(8) = x_8$ and $s(9) = x_9$ and $s(10) = x_{10}$ and $s(11) = x_{11}$ and $s(12) = x_{12}$ and $s(13) = x_{13}$ and $s(14) = x_{14}$ and $s(15) = x_{15}$ and $s(16) = x_{16}$.

(30) Let S be a non empty set and x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8, x_9, x_{10}, x_{11}, x_{12}, x_{13}, x_{14}, x_{15}, x_{16}, x_{17}, x_{18}, x_{19}, x_{20}, x_{21}, x_{22}, x_{23}, x_{24}, x_{25}, x_{26}, x_{27}, x_{28}, x_{29}, x_{30}, x_{31}, x_{32} be elements of S. Then there exists a finite sequence s of elements of S such that
s is 32-element and $s(1) = x_1$ and $s(2) = x_2$ and $s(3) = x_3$ and $s(4) = x_4$ and $s(5) = x_5$ and $s(6) = x_6$ and $s(7) = x_7$ and $s(8) = x_8$ and $s(9) = x_9$ and $s(10) = x_{10}$ and $s(11) = x_{11}$ and $s(12) = x_{12}$ and $s(13) = x_{13}$ and $s(14) = x_{14}$ and $s(15) = x_{15}$ and $s(16) = x_{16}$ and $s(17) = x_{17}$

and $s(18) = x_{18}$ and $s(19) = x_{19}$ and $s(20) = x_{20}$ and $s(21) = x_{21}$ and $s(22) = x_{22}$ and $s(23) = x_{23}$ and $s(24) = x_{24}$ and $s(25) = x_{25}$ and $s(26) = x_{26}$ and $s(27) = x_{27}$ and $s(28) = x_{28}$ and $s(29) = x_{29}$ and $s(30) = x_{30}$ and $s(31) = x_{31}$ and $s(32) = x_{32}$.

(31) Let S be a non empty set and x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8, x_9, x_{10}, x_{11}, x_{12}, x_{13}, x_{14}, x_{15}, x_{16}, x_{17}, x_{18}, x_{19}, x_{20}, x_{21}, x_{22}, x_{23}, x_{24}, x_{25}, x_{26}, x_{27}, x_{28}, x_{29}, x_{30}, x_{31}, x_{32}, x_{33}, x_{34}, x_{35}, x_{36}, x_{37}, x_{38}, x_{39}, x_{40}, x_{41}, x_{42}, x_{43}, x_{44}, x_{45}, x_{46}, x_{47}, x_{48} be elements of S. Then there exists a finite sequence s of elements of S such that

s is 48-element and $s(1) = x_1$ and $s(2) = x_2$ and $s(3) = x_3$ and $s(4) = x_4$ and $s(5) = x_5$ and $s(6) = x_6$ and $s(7) = x_7$ and $s(8) = x_8$ and $s(9) = x_9$ and $s(10) = x_{10}$ and $s(11) = x_{11}$ and $s(12) = x_{12}$ and $s(13) = x_{13}$ and $s(14) = x_{14}$ and $s(15) = x_{15}$ and $s(16) = x_{16}$ and $s(17) = x_{17}$ and $s(18) = x_{18}$ and $s(19) = x_{19}$ and $s(20) = x_{20}$ and $s(21) = x_{21}$ and $s(22) = x_{22}$ and $s(23) = x_{23}$ and $s(24) = x_{24}$ and $s(25) = x_{25}$ and $s(26) = x_{26}$ and $s(27) = x_{27}$ and $s(28) = x_{28}$ and $s(29) = x_{29}$ and $s(30) = x_{30}$ and $s(31) = x_{31}$ and $s(32) = x_{32}$ and $s(33) = x_{33}$ and $s(34) = x_{34}$ and $s(35) = x_{35}$ and $s(36) = x_{36}$ and $s(37) = x_{37}$ and $s(38) = x_{38}$ and $s(39) = x_{39}$ and $s(40) = x_{40}$ and $s(41) = x_{41}$ and $s(42) = x_{42}$ and $s(43) = x_{43}$ and $s(44) = x_{44}$ and $s(45) = x_{45}$ and $s(46) = x_{46}$ and $s(47) = x_{47}$ and $s(48) = x_{48}$.

(32) Let S be a non empty set and x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8, x_9, x_{10}, x_{11}, x_{12}, x_{13}, x_{14}, x_{15}, x_{16}, x_{17}, x_{18}, x_{19}, x_{20}, x_{21}, x_{22}, x_{23}, x_{24}, x_{25}, x_{26}, x_{27}, x_{28}, x_{29}, x_{30}, x_{31}, x_{32}, x_{33}, x_{34}, x_{35}, x_{36}, x_{37}, x_{38}, x_{39}, x_{40}, x_{41}, x_{42}, x_{43}, x_{44}, x_{45}, x_{46}, x_{47}, x_{48}, x_{49}, x_{50}, x_{51}, x_{52}, x_{53}, x_{54}, x_{55}, x_{56} be elements of S. Then there exists a finite sequence s of elements of S such that

s is 56-element and $s(1) = x_1$ and $s(2) = x_2$ and $s(3) = x_3$ and $s(4) = x_4$ and $s(5) = x_5$ and $s(6) = x_6$ and $s(7) = x_7$ and $s(8) = x_8$ and $s(9) = x_9$ and $s(10) = x_{10}$ and $s(11) = x_{11}$ and $s(12) = x_{12}$ and $s(13) = x_{13}$ and $s(14) = x_{14}$ and $s(15) = x_{15}$ and $s(16) = x_{16}$ and $s(17) = x_{17}$ and $s(18) = x_{18}$ and $s(19) = x_{19}$ and $s(20) = x_{20}$ and $s(21) = x_{21}$ and $s(22) = x_{22}$ and $s(23) = x_{23}$ and $s(24) = x_{24}$ and $s(25) = x_{25}$ and $s(26) = x_{26}$ and $s(27) = x_{27}$ and $s(28) = x_{28}$ and $s(29) = x_{29}$ and $s(30) = x_{30}$ and $s(31) = x_{31}$ and $s(32) = x_{32}$ and $s(33) = x_{33}$ and $s(34) = x_{34}$ and $s(35) = x_{35}$ and $s(36) = x_{36}$ and $s(37) = x_{37}$ and $s(38) = x_{38}$ and $s(39) = x_{39}$ and $s(40) = x_{40}$ and $s(41) = x_{41}$ and $s(42) = x_{42}$ and $s(43) = x_{43}$ and $s(44) = x_{44}$ and $s(45) = x_{45}$ and $s(46) = x_{46}$ and $s(47) = x_{47}$ and $s(48) = x_{48}$ and $s(49) = x_{49}$ and $s(50) = x_{50}$ and $s(51) = x_{51}$ and $s(52) = x_{52}$ and $s(53) = x_{53}$ and $s(54) = x_{54}$ and $s(55) = x_{55}$ and $s(56) = x_{56}$.

(33) Let S be a non empty set and x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8, x_9, x_{10}, x_{11},

x_{12}, x_{13}, x_{14}, x_{15}, x_{16}, x_{17}, x_{18}, x_{19}, x_{20}, x_{21}, x_{22}, x_{23}, x_{24}, x_{25}, x_{26}, x_{27}, x_{28}, x_{29}, x_{30}, x_{31}, x_{32}, x_{33}, x_{34}, x_{35}, x_{36}, x_{37}, x_{38}, x_{39}, x_{40}, x_{41}, x_{42}, x_{43}, x_{44}, x_{45}, x_{46}, x_{47}, x_{48}, x_{49}, x_{50}, x_{51}, x_{52}, x_{53}, x_{54}, x_{55}, x_{56}, x_{57}, x_{58}, x_{59}, x_{60}, x_{61}, x_{62}, x_{63}, x_{64} be elements of S. Then there exists a finite sequence s of elements of S such that

s is 64-element and $s(1) = x_1$ and $s(2) = x_2$ and $s(3) = x_3$ and $s(4) = x_4$ and $s(5) = x_5$ and $s(6) = x_6$ and $s(7) = x_7$ and $s(8) = x_8$ and $s(9) = x_9$ and $s(10) = x_{10}$ and $s(11) = x_{11}$ and $s(12) = x_{12}$ and $s(13) = x_{13}$ and $s(14) = x_{14}$ and $s(15) = x_{15}$ and $s(16) = x_{16}$ and $s(17) = x_{17}$ and $s(18) = x_{18}$ and $s(19) = x_{19}$ and $s(20) = x_{20}$ and $s(21) = x_{21}$ and $s(22) = x_{22}$ and $s(23) = x_{23}$ and $s(24) = x_{24}$ and $s(25) = x_{25}$ and $s(26) = x_{26}$ and $s(27) = x_{27}$ and $s(28) = x_{28}$ and $s(29) = x_{29}$ and $s(30) = x_{30}$ and $s(31) = x_{31}$ and $s(32) = x_{32}$ and $s(33) = x_{33}$ and $s(34) = x_{34}$ and $s(35) = x_{35}$ and $s(36) = x_{36}$ and $s(37) = x_{37}$ and $s(38) = x_{38}$ and $s(39) = x_{39}$ and $s(40) = x_{40}$ and $s(41) = x_{41}$ and $s(42) = x_{42}$ and $s(43) = x_{43}$ and $s(44) = x_{44}$ and $s(45) = x_{45}$ and $s(46) = x_{46}$ and $s(47) = x_{47}$ and $s(48) = x_{48}$ and $s(49) = x_{49}$ and $s(50) = x_{50}$ and $s(51) = x_{51}$ and $s(52) = x_{52}$ and $s(53) = x_{53}$ and $s(54) = x_{54}$ and $s(55) = x_{55}$ and $s(56) = x_{56}$ and $s(57) = x_{57}$ and $s(58) = x_{58}$ and $s(59) = x_{59}$ and $s(60) = x_{60}$ and $s(61) = x_{61}$ and $s(62) = x_{62}$ and $s(63) = x_{63}$ and $s(64) = x_{64}$.

Let n be a non empty natural number and let i be an element of n. We introduce $\mathrm{ntoSeg}\, i$ as a synonym of $\mathrm{succ}\, i$.

Let n be a non empty natural number and let i be an element of n. Then $\mathrm{ntoSeg}\, i$ is an element of $\mathrm{Seg}\, n$.

Let n be a non empty natural number and let f be a function from n into $\mathrm{Seg}\, n$. We say that f is NtoSeg if and only if:

(Def. 5) For every element i of n holds $f(i) = \mathrm{ntoSeg}\, i$.

Let n be a non empty natural number. One can check that there exists a function from n into $\mathrm{Seg}\, n$ which is NtoSeg.

Let n be a non empty natural number. Observe that every function from n into $\mathrm{Seg}\, n$ is bijective and NtoSeg.

We now state two propositions:

(34) Let n be a non empty natural number, f be an NtoSeg function from n into $\mathrm{Seg}\, n$, and i be a natural number. If $i < n$, then $f(i) = i + 1$ and $i \in \mathrm{dom}\, f$.

(35) Let S be a non empty set and x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8, x_9, x_{10}, x_{11}, x_{12}, x_{13}, x_{14}, x_{15}, x_{16}, x_{17}, x_{18}, x_{19}, x_{20}, x_{21}, x_{22}, x_{23}, x_{24}, x_{25}, x_{26}, x_{27}, x_{28}, x_{29}, x_{30}, x_{31}, x_{32}, x_{33}, x_{34}, x_{35}, x_{36}, x_{37}, x_{38}, x_{39}, x_{40}, x_{41}, x_{42}, x_{43}, x_{44}, x_{45}, x_{46}, x_{47}, x_{48}, x_{49}, x_{50}, x_{51}, x_{52}, x_{53}, x_{54}, x_{55}, x_{56}, x_{57}, x_{58}, x_{59}, x_{60}, x_{61}, x_{62}, x_{63}, x_{64} be elements of S. Then there exists a function f

from 64 into S such that
$f(0) = x_1$ and $f(1) = x_2$ and $f(2) = x_3$ and $f(3) = x_4$ and $f(4) = x_5$ and $f(5) = x_6$ and $f(6) = x_7$ and $f(7) = x_8$ and $f(8) = x_9$ and $f(9) = x_{10}$ and $f(10) = x_{11}$ and $f(11) = x_{12}$ and $f(12) = x_{13}$ and $f(13) = x_{14}$ and $f(14) = x_{15}$ and $f(15) = x_{16}$ and $f(16) = x_{17}$ and $f(17) = x_{18}$ and $f(18) = x_{19}$ and $f(19) = x_{20}$ and $f(20) = x_{21}$ and $f(21) = x_{22}$ and $f(22) = x_{23}$ and $f(23) = x_{24}$ and $f(24) = x_{25}$ and $f(25) = x_{26}$ and $f(26) = x_{27}$ and $f(27) = x_{28}$ and $f(28) = x_{29}$ and $f(29) = x_{30}$ and $f(30) = x_{31}$ and $f(31) = x_{32}$ and $f(32) = x_{33}$ and $f(33) = x_{34}$ and $f(34) = x_{35}$ and $f(35) = x_{36}$ and $f(36) = x_{37}$ and $f(37) = x_{38}$ and $f(38) = x_{39}$ and $f(39) = x_{40}$ and $f(40) = x_{41}$ and $f(41) = x_{42}$ and $f(42) = x_{43}$ and $f(43) = x_{44}$ and $f(44) = x_{45}$ and $f(45) = x_{46}$ and $f(46) = x_{47}$ and $f(47) = x_{48}$ and $f(48) = x_{49}$ and $f(49) = x_{50}$ and $f(50) = x_{51}$ and $f(51) = x_{52}$ and $f(52) = x_{53}$ and $f(53) = x_{54}$ and $f(54) = x_{55}$ and $f(55) = x_{56}$ and $f(56) = x_{57}$ and $f(57) = x_{58}$ and $f(58) = x_{59}$ and $f(59) = x_{60}$ and $f(60) = x_{61}$ and $f(61) = x_{62}$ and $f(62) = x_{63}$ and $f(63) = x_{64}$.

2. S-Boxes

The function DES-SBOX1 from 64 into 16 is defined by the conditions (Def. 6).

(Def. 6) (DES-SBOX1)(0) = 14 and (DES-SBOX1)(1) = 4 and (DES-SBOX1)(2) = 13 and (DES-SBOX1)(3) = 1 and (DES-SBOX1)(4) = 2 and (DES-SBOX1)(5) = 15 and (DES-SBOX1)(6) = 11 and (DES-SBOX1)(7) = 8 and (DES-SBOX1)(8) = 3 and (DES-SBOX1)(9) = 10 and (DES-SBOX1)(10) = 6 and (DES-SBOX1)(11) = 12 and (DES-SBOX1)(12) = 5 and (DES-SBOX1)(13) = 9 and (DES-SBOX1)(14) = 0 and (DES-SBOX1)(15) = 7 and (DES-SBOX1)(16) = 0 and (DES-SBOX1)(17) = 15 and (DES-SBOX1)(18) = 7 and (DES-SBOX1)(19) = 4 and (DES-SBOX1)(20) = 14 and (DES-SBOX1)(21) = 2 and (DES-SBOX1)(22) = 13 and (DES-SBOX1)(23) = 1 and (DES-SBOX1)(24) = 10 and (DES-SBOX1)(25) = 6 and (DES-SBOX1)(26) = 12 and (DES-SBOX1)(27) = 11 and (DES-SBOX1)(28) = 9 and (DES-SBOX1)(29) = 5 and (DES-SBOX1)(30) = 3 and (DES-SBOX1)(31) = 8 and (DES-SBOX1)(32) = 4 and (DES-SBOX1)(33) = 1 and (DES-SBOX1)(34) = 14 and (DES-SBOX1)(35) = 8 and (DES-SBOX1)(36) = 13 and (DES-SBOX1)(37) = 6 and (DES-SBOX1)(38) = 2 and (DES-SBOX1)(39) = 11 and (DES-SBOX1)(40) = 15 and (DES-SBOX1)(41) = 12 and (DES-SBOX1)(42) = 9 and (DES-SBOX1)(43) = 7 and

(DES-SBOX1)(44) = 3 and (DES-SBOX1)(45) = 10 and (DES-SBOX1)(46) = 5 and (DES-SBOX1)(47) = 0 and (DES-SBOX1)(48) = 15 and (DES-SBOX1)(49) = 12 and (DES-SBOX1)(50) = 8 and (DES-SBOX1)(51) = 2 and (DES-SBOX1)(52) = 4 and (DES-SBOX1)(53) = 9 and (DES-SBOX1)(54) = 1 and (DES-SBOX1)(55) = 7 and (DES-SBOX1)(56) = 5 and (DES-SBOX1)(57) = 11 and (DES-SBOX1)(58) = 3 and (DES-SBOX1)(59) = 14 and (DES-SBOX1)(60) = 10 and (DES-SBOX1)(61) = 0 and (DES-SBOX1)(62) = 6 and (DES-SBOX1)(63) = 13.

The function DES-SBOX2 from 64 into 16 is defined by the conditions (Def. 7).

(Def. 7) (DES-SBOX2)(0) = 15 and (DES-SBOX2)(1) = 1 and (DES-SBOX2)(2) = 8 and (DES-SBOX2)(3) = 14 and (DES-SBOX2)(4) = 6 and (DES-SBOX2)(5) = 11 and (DES-SBOX2)(6) = 3 and (DES-SBOX2)(7) = 4 and (DES-SBOX2)(8) = 9 and (DES-SBOX2)(9) = 7 and (DES-SBOX2)(10) = 2 and (DES-SBOX2)(11) = 13 and (DES-SBOX2)(12) = 12 and (DES-SBOX2)(13) = 0 and (DES-SBOX2)(14) = 5 and (DES-SBOX2)(15) = 10 and (DES-SBOX2)(16) = 3 and (DES-SBOX2)(17) = 13 and (DES-SBOX2)(18) = 4 and (DES-SBOX2)(19) = 7 and (DES-SBOX2)(20) = 15 and (DES-SBOX2)(21) = 2 and (DES-SBOX2)(22) = 8 and (DES-SBOX2)(23) = 14 and (DES-SBOX2)(24) = 12 and (DES-SBOX2)(25) = 0 and (DES-SBOX2)(26) = 1 and (DES-SBOX2)(27) = 10 and (DES-SBOX2)(28) = 6 and (DES-SBOX2)(29) = 9 and (DES-SBOX2)(30) = 11 and (DES-SBOX2)(31) = 5 and (DES-SBOX2)(32) = 0 and (DES-SBOX2)(33) = 14 and (DES-SBOX2)(34) = 7 and (DES-SBOX2)(35) = 11 and (DES-SBOX2)(36) = 10 and (DES-SBOX2)(37) = 4 and (DES-SBOX2)(38) = 13 and (DES-SBOX2)(39) = 1 and (DES-SBOX2)(40) = 5 and (DES-SBOX2)(41) = 8 and (DES-SBOX2)(42) = 12 and (DES-SBOX2)(43) = 6 and (DES-SBOX2)(44) = 9 and (DES-SBOX2)(45) = 3 and (DES-SBOX2)(46) = 2 and (DES-SBOX2)(47) = 15 and (DES-SBOX2)(48) = 13 and (DES-SBOX2)(49) = 8 and (DES-SBOX2)(50) = 10 and (DES-SBOX2)(51) = 1 and (DES-SBOX2)(52) = 3 and (DES-SBOX2)(53) = 15 and (DES-SBOX2)(54) = 4 and (DES-SBOX2)(55) = 2 and (DES-SBOX2)(56) = 11 and (DES-SBOX2)(57) = 6 and (DES-SBOX2)(58) = 7 and (DES-SBOX2)(59) = 12 and (DES-SBOX2)(60) = 0 and (DES-SBOX2)(61) = 5 and (DES-SBOX2)(62) = 14 and (DES-SBOX2)(63) = 9.

The function DES-SBOX3 from 64 into 16 is defined by the conditions (Def. 8).

(Def. 8) (DES-SBOX3)(0) = 10 and (DES-SBOX3)(1) = 0 and (DES-SBOX3)(2) = 9 and (DES-SBOX3)(3) = 14 and (DES-SBOX3)(4) = 6 and (DES-SBOX3)(5) = 3 and (DES-SBOX3)(6) = 15 and (DES-SBOX3)(7) = 5 and (DES-SBOX3)(8) = 1 and (DES-SBOX3)(9) = 13 and (DES-SBOX3)(10) = 12 and (DES-SBOX3)(11) = 7 and (DES-SBOX3)(12) = 11 and (DES-SBOX3)(13) = 4 and (DES-SBOX3)(14) = 2 and (DES-SBOX3)(15) = 8 and (DES-SBOX3)(16) = 13 and (DES-SBOX3)(17) = 7 and (DES-SBOX3)(18) = 0 and (DES-SBOX3)(19) = 9 and (DES-SBOX3)(20) = 3 and (DES-SBOX3)(21) = 4 and (DES-SBOX3)(22) = 6 and (DES-SBOX3)(23) = 10 and (DES-SBOX3)(24) = 2 and (DES-SBOX3)(25) = 8 and (DES-SBOX3)(26) = 5 and (DES-SBOX3)(27) = 14 and (DES-SBOX3)(28) = 12 and (DES-SBOX3)(29) = 11 and (DES-SBOX3)(30) = 15 and (DES-SBOX3)(31) = 1 and (DES-SBOX3)(32) = 13 and (DES-SBOX3)(33) = 6 and (DES-SBOX3)(34) = 4 and (DES-SBOX3)(35) = 9 and (DES-SBOX3)(36) = 8 and (DES-SBOX3)(37) = 15 and (DES-SBOX3)(38) = 3 and (DES-SBOX3)(39) = 0 and (DES-SBOX3)(40) = 11 and (DES-SBOX3)(41) = 1 and (DES-SBOX3)(42) = 2 and (DES-SBOX3)(43) = 12 and (DES-SBOX3)(44) = 5 and (DES-SBOX3)(45) = 10 and (DES-SBOX3)(46) = 14 and (DES-SBOX3)(47) = 7 and (DES-SBOX3)(48) = 1 and (DES-SBOX3)(49) = 10 and (DES-SBOX3)(50) = 13 and (DES-SBOX3)(51) = 0 and (DES-SBOX3)(52) = 6 and (DES-SBOX3)(53) = 9 and (DES-SBOX3)(54) = 8 and (DES-SBOX3)(55) = 7 and (DES-SBOX3)(56) = 4 and (DES-SBOX3)(57) = 15 and (DES-SBOX3)(58) = 14 and (DES-SBOX3)(59) = 3 and (DES-SBOX3)(60) = 11 and (DES-SBOX3)(61) = 5 and (DES-SBOX3)(62) = 2 and (DES-SBOX3)(63) = 12.

The function DES-SBOX4 from 64 into 16 is defined by the conditions (Def. 9).

(Def. 9) (DES-SBOX4)(0) = 7 and (DES-SBOX4)(1) = 13 and (DES-SBOX4)(2) = 14 and (DES-SBOX4)(3) = 3 and (DES-SBOX4)(4) = 0 and (DES-SBOX4)(5) = 6 and (DES-SBOX4)(6) = 9 and (DES-SBOX4)(7) = 10 and (DES-SBOX4)(8) = 1 and (DES-SBOX4)(9) = 2 and (DES-SBOX4)(10) = 8 and (DES-SBOX4)(11) = 5 and (DES-SBOX4)(12) = 11 and (DES-SBOX4)(13) = 12 and (DES-SBOX4)(14) = 4 and (DES-SBOX4)(15) = 15 and (DES-SBOX4)(16) = 13 and (DES-SBOX4)(17) = 8 and (DES-SBOX4)(18) = 11 and (DES-SBOX4)(19) = 5 and (DES-SBOX4)(20) = 6 and (DES-SBOX4)(21) = 15 and (DES-SBOX4)(22) = 0 and (DES-SBOX4)(23) = 3 and (DES-SBOX4)(24) = 4 and (DES-SBOX4)(25) = 7 and (DES-SBOX4)(26) = 2 and (DES-SBOX4)(27) = 12 and (DES-SBOX4)(28) = 1 and (DES-SBOX4)(29) = 10 and (DES-SBOX4)(30) = 14 and (DES-SBOX4)(31) = 9 and (DES-SBOX4)(32) = 10 and (DES-SBOX4)(33) = 6 and (DES-SBOX4)(34) = 9 and (DES-SBOX4)(35) = 0 and (DES-SBOX4)(36) = 12 and (DES-SBOX4)(37) = 11 and (DES-SBOX4)(38) = 7 and (DES-SBOX4)(39) = 13 and (DES-SBOX4)(40) = 15 and (DES-SBOX4)(41) = 1 and (DES-SBOX4)(42) = 3 and (DES-SBOX4)(43) = 14 and (DES-SBOX4)(44) = 5 and (DES-SBOX4)(45) = 2 and (DES-SBOX4)(46) = 8 and (DES-SBOX4)(47) = 4 and (DES-SBOX4)(48) = 3 and (DES-SBOX4)(49) = 15 and (DES-SBOX4)(50) = 0 and (DES-SBOX4)(51) = 6 and (DES-SBOX4)(52) = 10 and (DES-SBOX4)(53) = 1 and (DES-SBOX4)(54) = 13 and (DES-SBOX4)(55) = 8 and (DES-SBOX4)(56) = 9 and (DES-SBOX4)(57) = 4 and (DES-SBOX4)(58) = 5 and (DES-SBOX4)(59) = 11 and (DES-SBOX4)(60) = 12 and (DES-SBOX4)(61) = 7 and (DES-SBOX4)(62) = 2 and (DES-SBOX4)(63) = 14.

The function DES-SBOX5 from 64 into 16 is defined by the conditions (Def. 10).

(Def. 10) (DES-SBOX5)(0) = 2 and (DES-SBOX5)(1) = 12 and (DES-SBOX5)(2) = 4 and (DES-SBOX5)(3) = 1 and (DES-SBOX5)(4) = 7 and (DES-SBOX5)(5) = 10 and (DES-SBOX5)(6) = 11 and (DES-SBOX5)(7) = 6 and (DES-SBOX5)(8) = 8 and (DES-SBOX5)(9) = 5 and (DES-SBOX5)(10) = 3 and (DES-SBOX5)(11) = 15 and (DES-SBOX5)(12) = 13 and (DES-SBOX5)(13) = 0 and (DES-SBOX5)(14) = 14 and (DES-SBOX5)(15) = 9 and (DES-SBOX5)(16) = 14 and (DES-SBOX5)(17) = 11 and (DES-SBOX5)(18) = 2 and (DES-SBOX5)(19) = 12 and (DES-SBOX5)(20) = 4 and (DES-SBOX5)(21) = 7 and (DES-SBOX5)(22) = 13 and (DES-SBOX5)(23) = 1 and (DES-SBOX5)(24) = 5 and (DES-SBOX5)(25) = 0 and (DES-SBOX5)(26) = 15 and (DES-SBOX5)(27) = 10 and (DES-SBOX5)(28) = 3 and (DES-SBOX5)(29) = 9 and (DES-SBOX5)(30) = 8 and (DES-SBOX5)(31) = 6 and (DES-SBOX5)(32) = 4 and (DES-SBOX5)(33) = 2 and (DES-SBOX5)(34) = 1 and (DES-SBOX5)(35) = 11 and (DES-SBOX5)(36) = 10 and (DES-SBOX5)(37) = 13 and (DES-SBOX5)(38) = 7 and (DES-SBOX5)(39) = 8 and (DES-SBOX5)(40) = 15 and (DES-SBOX5)(41) = 9 and (DES-SBOX5)(42) = 12 and (DES-SBOX5)(43) = 5 and (DES-SBOX5)(44) = 6 and (DES-SBOX5)(45) = 3 and (DES-SBOX5)(46) = 0 and (DES-SBOX5)(47) = 14 and (DES-SBOX5)(48) = 11 and (DES-SBOX5)(49) = 8 and (DES-SBOX5)(50) = 12 and (DES-SBOX5)(51) =

7 and (DES-SBOX5)(52) = 1 and (DES-SBOX5)(53) = 14 and (DES-SBOX5)(54) = 2 and (DES-SBOX5)(55) = 13 and (DES-SBOX5)(56) = 6 and (DES-SBOX5)(57) = 15 and (DES-SBOX5)(58) = 0 and (DES-SBOX5)(59) = 9 and (DES-SBOX5)(60) = 10 and (DES-SBOX5)(61) = 4 and (DES-SBOX5)(62) = 5 and (DES-SBOX5)(63) = 3.

The function DES-SBOX6 from 64 into 16 is defined by the conditions (Def. 11).

(Def. 11) (DES-SBOX6)(0) = 12 and (DES-SBOX6)(1) = 1 and (DES-SBOX6)(2) = 10 and (DES-SBOX6)(3) = 15 and (DES-SBOX6)(4) = 9 and (DES-SBOX6)(5) = 2 and (DES-SBOX6)(6) = 6 and (DES-SBOX6)(7) = 8 and (DES-SBOX6)(8) = 0 and (DES-SBOX6)(9) = 13 and (DES-SBOX6)(10) = 3 and (DES-SBOX6)(11) = 4 and (DES-SBOX6)(12) = 14 and (DES-SBOX6)(13) = 7 and (DES-SBOX6)(14) = 5 and (DES-SBOX6)(15) = 11 and (DES-SBOX6)(16) = 10 and (DES-SBOX6)(17) = 15 and (DES-SBOX6)(18) = 4 and (DES-SBOX6)(19) = 2 and (DES-SBOX6)(20) = 7 and (DES-SBOX6)(21) = 12 and (DES-SBOX6)(22) = 9 and (DES-SBOX6)(23) = 5 and (DES-SBOX6)(24) = 6 and (DES-SBOX6)(25) = 1 and (DES-SBOX6)(26) = 13 and (DES-SBOX6)(27) = 14 and (DES-SBOX6)(28) = 0 and (DES-SBOX6)(29) = 11 and (DES-SBOX6)(30) = 3 and (DES-SBOX6)(31) = 8 and (DES-SBOX6)(32) = 9 and (DES-SBOX6)(33) = 14 and (DES-SBOX6)(34) = 15 and (DES-SBOX6)(35) = 5 and (DES-SBOX6)(36) = 2 and (DES-SBOX6)(37) = 8 and (DES-SBOX6)(38) = 12 and (DES-SBOX6)(39) = 3 and (DES-SBOX6)(40) = 7 and (DES-SBOX6)(41) = 0 and (DES-SBOX6)(42) = 4 and (DES-SBOX6)(43) = 10 and (DES-SBOX6)(44) = 1 and (DES-SBOX6)(45) = 13 and (DES-SBOX6)(46) = 11 and (DES-SBOX6)(47) = 6 and (DES-SBOX6)(48) = 4 and (DES-SBOX6)(49) = 3 and (DES-SBOX6)(50) = 2 and (DES-SBOX6)(51) = 12 and (DES-SBOX6)(52) = 9 and (DES-SBOX6)(53) = 5 and (DES-SBOX6)(54) = 15 and (DES-SBOX6)(55) = 10 and (DES-SBOX6)(56) = 11 and (DES-SBOX6)(57) = 14 and (DES-SBOX6)(58) = 1 and (DES-SBOX6)(59) = 7 and (DES-SBOX6)(60) = 6 and (DES-SBOX6)(61) = 0 and (DES-SBOX6)(62) = 8 and (DES-SBOX6)(63) = 13.

The function DES-SBOX7 from 64 into 16 is defined by the conditions (Def. 12).

(Def. 12) (DES-SBOX7)(0) = 4 and (DES-SBOX7)(1) = 11 and (DES-SBOX7)(2) = 2 and (DES-SBOX7)(3) = 14 and (DES-SBOX7)(4) = 15 and (DES-SBOX7)(5) = 0 and (DES-SBOX7)(6) = 8 and (DES-SBOX7)(7) =

13 and (DES-SBOX7)(8) = 3 and (DES-SBOX7)(9) = 12 and (DES-SBOX7)(10) = 9 and (DES-SBOX7)(11) = 7 and (DES-SBOX7)(12) = 5 and (DES-SBOX7)(13) = 10 and (DES-SBOX7)(14) = 6 and (DES-SBOX7)(15) = 1 and (DES-SBOX7)(16) = 13 and (DES-SBOX7)(17) = 0 and (DES-SBOX7)(18) = 11 and (DES-SBOX7)(19) = 7 and (DES-SBOX7)(20) = 4 and (DES-SBOX7)(21) = 9 and (DES-SBOX7)(22) = 1 and (DES-SBOX7)(23) = 10 and (DES-SBOX7)(24) = 14 and (DES-SBOX7)(25) = 3 and (DES-SBOX7)(26) = 5 and (DES-SBOX7)(27) = 12 and (DES-SBOX7)(28) = 2 and (DES-SBOX7)(29) = 15 and (DES-SBOX7)(30) = 8 and (DES-SBOX7)(31) = 6 and (DES-SBOX7)(32) = 1 and (DES-SBOX7)(33) = 4 and (DES-SBOX7)(34) = 11 and (DES-SBOX7)(35) = 13 and (DES-SBOX7)(36) = 12 and (DES-SBOX7)(37) = 3 and (DES-SBOX7)(38) = 7 and (DES-SBOX7)(39) = 14 and (DES-SBOX7)(40) = 10 and (DES-SBOX7)(41) = 15 and (DES-SBOX7)(42) = 6 and (DES-SBOX7)(43) = 8 and (DES-SBOX7)(44) = 0 and (DES-SBOX7)(45) = 5 and (DES-SBOX7)(46) = 9 and (DES-SBOX7)(47) = 2 and (DES-SBOX7)(48) = 6 and (DES-SBOX7)(49) = 11 and (DES-SBOX7)(50) = 13 and (DES-SBOX7)(51) = 8 and (DES-SBOX7)(52) = 1 and (DES-SBOX7)(53) = 4 and (DES-SBOX7)(54) = 10 and (DES-SBOX7)(55) = 7 and (DES-SBOX7)(56) = 9 and (DES-SBOX7)(57) = 5 and (DES-SBOX7)(58) = 0 and (DES-SBOX7)(59) = 15 and (DES-SBOX7)(60) = 14 and (DES-SBOX7)(61) = 2 and (DES-SBOX7)(62) = 3 and (DES-SBOX7)(63) = 12.

The function DES-SBOX8 from 64 into 16 is defined by the conditions (Def. 13).

(Def. 13) (DES-SBOX8)(0) = 13 and (DES-SBOX8)(1) = 2 and (DES-SBOX8)(2) = 8 and (DES-SBOX8)(3) = 4 and (DES-SBOX8)(4) = 6 and (DES-SBOX8)(5) = 15 and (DES-SBOX8)(6) = 11 and (DES-SBOX8)(7) = 1 and (DES-SBOX8)(8) = 10 and (DES-SBOX8)(9) = 9 and (DES-SBOX8)(10) = 3 and (DES-SBOX8)(11) = 14 and (DES-SBOX8)(12) = 5 and (DES-SBOX8)(13) = 0 and (DES-SBOX8)(14) = 12 and (DES-SBOX8)(15) = 7 and (DES-SBOX8)(16) = 1 and (DES-SBOX8)(17) = 15 and (DES-SBOX8)(18) = 13 and (DES-SBOX8)(19) = 8 and (DES-SBOX8)(20) = 10 and (DES-SBOX8)(21) = 3 and (DES-SBOX8)(22) = 7 and (DES-SBOX8)(23) = 4 and (DES-SBOX8)(24) = 12 and (DES-SBOX8)(25) = 5 and (DES-SBOX8)(26) = 5 and (DES-SBOX8)(27) = 11 and (DES-SBOX8)(28) = 0 and (DES-SBOX8)(29) = 14 and (DES-SBOX8)(30) = 9 and (DES-SBOX8)(31) = 2 and (DES-SBOX8)(32) = 7 and (DES-SBOX8)(33) = 11 and (DES-SBOX8)(34) = 4 and (DES-SBOX8)(35) = 1 and (DES-SBOX8)(36) = 9 and (DES-SBOX8)(37) = 12 and (DES-SBOX8)(38) = 14 and (DES-SBOX8)(39) = 2 and (DES-SBOX8)(40) = 0 and (DES-SBOX8)(41) = 6 and (DES-SBOX8)(42) = 10 and (DES-SBOX8)(43) = 13 and (DES-SBOX8)(44) = 15 and (DES-SBOX8)(45) = 3 and (DES-SBOX8)(46) = 5 and (DES-SBOX8)(47) = 8 and (DES-SBOX8)(48) = 2 and (DES-SBOX8)(49) = 1 and (DES-SBOX8)(50) = 14 and (DES-SBOX8)(51) = 7 and (DES-SBOX8)(52) = 4 and (DES-SBOX8)(53) = 10 and (DES-SBOX8)(54) = 8 and (DES-SBOX8)(55) = 13 and (DES-SBOX8)(56) = 15 and (DES-SBOX8)(57) = 12 and (DES-SBOX8)(58) = 9 and (DES-SBOX8)(59) = 0 and (DES-SBOX8)(60) = 3 and (DES-SBOX8)(61) = 5 and (DES-SBOX8)(62) = 6 and (DES-SBOX8)(63) = 11.

3. Initial Permutation

Let r be an element of *Boolean*^{64}. The functor DES-IP r yields an element of *Boolean*^{64} and is defined by the conditions (Def. 14).

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

and $(\text{DES-IP}\,r)(53) = r(29)$ and $(\text{DES-IP}\,r)(54) = r(21)$ and $(\text{DES-IP}\,r)(55) = r(13)$ and $(\text{DES-IP}\,r)(56) = r(5)$ and $(\text{DES-IP}\,r)(57) = r(63)$ and $(\text{DES-IP}\,r)(58) = r(55)$ and $(\text{DES-IP}\,r)(59) = r(47)$ and $(\text{DES-IP}\,r)(60) = r(39)$ and $(\text{DES-IP}\,r)(61) = r(31)$ and $(\text{DES-IP}\,r)(62) = r(23)$ and $(\text{DES-IP}\,r)(63) = r(15)$ and $(\text{DES-IP}\,r)(64) = r(7)$.

The function DES-PIP from $\mathit{Boolean}^{64}$ into $\mathit{Boolean}^{64}$ is defined by:

(Def. 15) For every element i of $\mathit{Boolean}^{64}$ holds $(\text{DES-PIP})(i) = \text{DES-IP}\,i$.

Let r be an element of $\mathit{Boolean}^{64}$. The functor DES-IPINV r yields an element of $\mathit{Boolean}^{64}$ and is defined by the conditions (Def. 16).

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

(DES-IPINV r)(63) = r(57) and (DES-IPINV r)(64) = r(25).

The function DES-PIPINV from $Boolean^{64}$ into $Boolean^{64}$ is defined by:

(Def. 17) For every element i of $Boolean^{64}$ holds (DES-PIPINV)(i) = DES-IPINV i.

Let us note that DES-PIP is bijective.

Let us note that DES-PIPINV is bijective.

The following proposition is true

(36) DES-PIPINV = $(\text{DES-PIP})^{-1}$.

4. Feistel Function

Let r be an element of $Boolean^{32}$. The functor DES-E r yielding an element of $Boolean^{48}$ is defined by the conditions (Def. 18).

(Def. 18) (DES-E r)(1) = r(32) and (DES-E r)(2) = r(1) and (DES-E r)(3) = r(2) and (DES-E r)(4) = r(3) and (DES-E r)(5) = r(4) and (DES-E r)(6) = r(5) and (DES-E r)(7) = r(4) and (DES-E r)(8) = r(5) and (DES-E r)(9) = r(6) and (DES-E r)(10) = r(7) and (DES-E r)(11) = r(8) and (DES-E r)(12) = r(9) and (DES-E r)(13) = r(8) and (DES-E r)(14) = r(9) and (DES-E r)(15) = r(10) and (DES-E r)(16) = r(11) and (DES-E r)(17) = r(12) and (DES-E r)(18) = r(13) and (DES-E r)(19) = r(12) and (DES-E r)(20) = r(13) and (DES-E r)(21) = r(14) and (DES-E r)(22) = r(15) and (DES-E r)(23) = r(16) and (DES-E r)(24) = r(17) and (DES-E r)(25) = r(16) and (DES-E r)(26) = r(17) and (DES-E r)(27) = r(18) and (DES-E r)(28) = r(19) and (DES-E r)(29) = r(20) and (DES-E r)(30) = r(21) and (DES-E r)(31) = r(20) and (DES-E r)(32) = r(21) and (DES-E r)(33) = r(22) and (DES-E r)(34) = r(23) and (DES-E r)(35) = r(24) and (DES-E r)(36) = r(25) and (DES-E r)(37) = r(24) and (DES-E r)(38) = r(25) and (DES-E r)(39) = r(26) and (DES-E r)(40) = r(27) and (DES-E r)(41) = r(28) and (DES-E r)(42) = r(29) and (DES-E r)(43) = r(28) and (DES-E r)(44) = r(29) and (DES-E r)(45) = r(30) and (DES-E r)(46) = r(31) and (DES-E r)(47) = r(32) and (DES-E r)(48) = r(1).

Let r be an element of $Boolean^{32}$. The functor DES-P r yielding an element of $Boolean^{32}$ is defined by the conditions (Def. 19).

(Def. 19) (DES-P r)(1) = r(16) and (DES-P r)(2) = r(7) and (DES-P r)(3) = r(20) and (DES-P r)(4) = r(21) and (DES-P r)(5) = r(29) and (DES-P r)(6) = r(12) and (DES-P r)(7) = r(28) and (DES-P r)(8) = r(17) and (DES-P r)(9) = r(1) and (DES-P r)(10) = r(15) and (DES-P r)(11) = r(23) and (DES-P r)(12) = r(26) and (DES-P r)(13) = r(5) and (DES-P r)(14) = r(18) and (DES-P r)(15) = r(31) and

(DES-P r)(16) = r(10) and (DES-P r)(17) = r(2) and (DES-P r)(18) = r(8) and (DES-P r)(19) = r(24) and (DES-P r)(20) = r(14) and (DES-P r)(21) = r(32) and (DES-P r)(22) = r(27) and (DES-P r)(23) = r(3) and (DES-P r)(24) = r(9) and (DES-P r)(25) = r(19) and (DES-P r)(26) = r(13) and (DES-P r)(27) = r(30) and (DES-P r)(28) = r(6) and (DES-P r)(29) = r(22) and (DES-P r)(30) = r(11) and (DES-P r)(31) = r(4) and (DES-P r)(32) = r(25).

Let r be an element of $\mathit{Boolean}^{48}$. The functor DES-DIV8 r yielding an element of $(\mathit{Boolean}^6)^8$ is defined by the conditions (Def. 20).

(Def. 20) (DES-DIV8 r)(1) = Op-Left($r, 6$) and (DES-DIV8 r)(2) = Op-Left(Op-Right($r, 6$), 6) and (DES-DIV8 r)(3) = Op-Left(Op-Right($r, 12$), 6) and (DES-DIV8 r)(4) = Op-Left(Op-Right($r, 18$), 6) and (DES-DIV8 r)(5) = Op-Left(Op-Right($r, 24$), 6) and (DES-DIV8 r)(6) = Op-Left(Op-Right($r, 30$), 6) and (DES-DIV8 r)(7) = Op-Left(Op-Right($r, 36$), 6) and (DES-DIV8 r)(8) = Op-Right($r, 42$).

Next we state the proposition

(37) Let r be an element of $\mathit{Boolean}^{48}$. Then there exist elements s_1, s_2, s_3, s_4, s_5, s_6, s_7, s_8 of $\mathit{Boolean}^6$ such that s_1 = (DES-DIV8 r)(1) and s_2 = (DES-DIV8 r)(2) and s_3 = (DES-DIV8 r)(3) and s_4 = (DES-DIV8 r)(4) and s_5 = (DES-DIV8 r)(5) and s_6 = (DES-DIV8 r)(6) and s_7 = (DES-DIV8 r)(7) and s_8 = (DES-DIV8 r)(8) and $r = s_1 \frown s_2 \frown s_3 \frown s_4 \frown s_5 \frown s_6 \frown s_7 \frown s_8$.

Let t be an element of $\mathit{Boolean}^6$. The functor B6toN64 t yielding an element of 64 is defined by:

(Def. 21) B6toN64 $t = 32 \cdot t(1) + 16 \cdot t(6) + 8 \cdot t(2) + 4 \cdot t(3) + 2 \cdot t(4) + 1 \cdot t(5)$.

The function N16toB4 from 16 into $\mathit{Boolean}^4$ is defined by the conditions (Def. 22).

(Def. 22) (N16toB4)(0) = $\langle 0,0,0,0 \rangle$ and (N16toB4)(1) = $\langle 0,0,0,1 \rangle$ and (N16toB4)(2) = $\langle 0,0,1,0 \rangle$ and (N16toB4)(3) = $\langle 0,0,1,1 \rangle$ and (N16toB4)(4) = $\langle 0,1,0,0 \rangle$ and (N16toB4)(5) = $\langle 0,1,0,1 \rangle$ and (N16toB4)(6) = $\langle 0,1,1,0 \rangle$ and (N16toB4)(7) = $\langle 0,1,1,1 \rangle$ and (N16toB4)(8) = $\langle 1,0,0,0 \rangle$ and (N16toB4)(9) = $\langle 1,0,0,1 \rangle$ and (N16toB4)(10) = $\langle 1,0,1,0 \rangle$ and (N16toB4)(11) = $\langle 1,0,1,1 \rangle$ and (N16toB4)(12) = $\langle 1,1,0,0 \rangle$ and (N16toB4)(13) = $\langle 1,1,0,1 \rangle$ and (N16toB4)(14) = $\langle 1,1,1,0 \rangle$ and (N16toB4)(15) = $\langle 1,1,1,1 \rangle$.

Let R be an element of $\mathit{Boolean}^{32}$ and let R_2 be an element of $\mathit{Boolean}^{48}$. The functor DES-F(R, R_2) yields an element of $\mathit{Boolean}^{32}$ and is defined by the condition (Def. 23).

(Def. 23) There exist elements D_1, D_2, D_3, D_4, D_5, D_6, D_7, D_8 of $\mathit{Boolean}^6$ and

there exist elements x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8 of $Boolean^4$ and there exists an element C_{32} of $Boolean^{32}$ such that
$D_1 =$ (DES-DIV8 Op-XOR(DES-E R, R_2))(1) and
$D_2 =$ (DES-DIV8 Op-XOR(DES-E R, R_2))(2) and
$D_3 =$ (DES-DIV8 Op-XOR(DES-E R, R_2))(3) and
$D_4 =$ (DES-DIV8 Op-XOR(DES-E R, R_2))(4) and
$D_5 =$ (DES-DIV8 Op-XOR(DES-E R, R_2))(5) and
$D_6 =$ (DES-DIV8 Op-XOR(DES-E R, R_2))(6) and
$D_7 =$ (DES-DIV8 Op-XOR(DES-E R, R_2))(7) and
$D_8 =$ (DES-DIV8 Op-XOR(DES-E R, R_2))(8) and
Op-XOR(DES-E R, R_2) $= D_1 \frown D_2 \frown D_3 \frown D_4 \frown D_5 \frown D_6 \frown D_7 \frown D_8$ and $x_1 =$ (N16toB4)((DES-SBOX1)(B6toN64 D_1)) and $x_2 =$ (N16toB4)((DES-SBOX2)(B6toN64 D_2)) and
$x_3 =$ (N16toB4)((DES-SBOX3)(B6toN64 D_3)) and
$x_4 =$ (N16toB4)((DES-SBOX4)(B6toN64 D_4)) and
$x_5 =$ (N16toB4)((DES-SBOX5)(B6toN64 D_5)) and
$x_6 =$ (N16toB4)((DES-SBOX6)(B6toN64 D_6)) and
$x_7 =$ (N16toB4)((DES-SBOX7)(B6toN64 D_7)) and
$x_8 =$ (N16toB4)((DES-SBOX8)(B6toN64 D_8)) and $C_{32} = x_1 \frown x_2 \frown x_3 \frown x_4 \frown x_5 \frown x_6 \frown x_7 \frown x_8$ and DES-F$(R, R_2) =$ DES-P C_{32}.

The function DES-FFUNC from $Boolean^{32} \times Boolean^{48}$ into $Boolean^{32}$ is defined as follows:

(Def. 24) For every element z of $Boolean^{32} \times Boolean^{48}$ holds (DES-FFUNC)$(z) =$ DES-F$(z_{\mathbf{1}}, z_{\mathbf{2}})$.

5. Key Schedule

Let r be an element of $Boolean^{64}$. The functor DES-PC1 r yields an element of $Boolean^{56}$ and is defined by the conditions (Def. 25).

(Def. 25) (DES-PC1 r)(1) $= r(57)$ and (DES-PC1 r)(2) $= r(49)$ and (DES-PC1 r)(3) $= r(41)$ and (DES-PC1 r)(4) $= r(33)$ and (DES-PC1 r)(5) $= r(25)$ and (DES-PC1 r)(6) $= r(17)$ and (DES-PC1 r)(7) $= r(9)$ and (DES-PC1 r)(8) $= r(1)$ and (DES-PC1 r)(9) $= r(58)$ and (DES-PC1 r)(10) $= r(50)$ and (DES-PC1 r)(11) $= r(42)$ and (DES-PC1 r)(12) $= r(34)$ and (DES-PC1 r)(13) $= r(26)$ and (DES-PC1 r)(14) $= r(18)$ and (DES-PC1 r)(15) $= r(10)$ and (DES-PC1 r)(16) $= r(2)$ and (DES-PC1 r)(17) $= r(59)$ and (DES-PC1 r)(18) $= r(51)$ and (DES-PC1 r)(19) $= r(43)$ and (DES-PC1 r)(20) $= r(35)$ and (DES-PC1 r)(21) $= r(27)$ and (DES-PC1 r)(22) $= r(19)$ and (DES-PC1 r)(23) $= r(11)$ and (DES-PC1 r)(24) $= r(3)$ and (DES-PC1 r)(25) $= r(60)$ and

(DES-PC1 r)(26) = r(52) and (DES-PC1 r)(27) = r(44) and (DES-PC1 r)(28) = r(36) and (DES-PC1 r)(29) = r(63) and (DES-PC1 r)(30) = r(55) and (DES-PC1 r)(31) = r(47) and (DES-PC1 r)(32) = r(39) and (DES-PC1 r)(33) = r(31) and (DES-PC1 r)(34) = r(23) and (DES-PC1 r)(35) = r(15) and (DES-PC1 r)(36) = r(7) and (DES-PC1 r)(37) = r(62) and (DES-PC1 r)(38) = r(54) and (DES-PC1 r)(39) = r(46) and (DES-PC1 r)(40) = r(38) and (DES-PC1 r)(41) = r(30) and (DES-PC1 r)(42) = r(22) and (DES-PC1 r)(43) = r(14) and (DES-PC1 r)(44) = r(6) and (DES-PC1 r)(45) = r(61) and (DES-PC1 r)(46) = r(53) and (DES-PC1 r)(47) = r(45) and (DES-PC1 r)(48) = r(37) and (DES-PC1 r)(49) = r(29) and (DES-PC1 r)(50) = r(21) and (DES-PC1 r)(51) = r(13) and (DES-PC1 r)(52) = r(5) and (DES-PC1 r)(53) = r(28) and (DES-PC1 r)(54) = r(20) and (DES-PC1 r)(55) = r(12) and (DES-PC1 r)(56) = r(4).

Let r be an element of *Boolean*^{56}. The functor DES-PC2 r yielding an element of *Boolean*^{48} is defined by the conditions (Def. 26).

(Def. 26) (DES-PC2 r)(1) = r(14) and (DES-PC2 r)(2) = r(17) and (DES-PC2 r)(3) = r(11) and (DES-PC2 r)(4) = r(24) and (DES-PC2 r)(5) = r(1) and (DES-PC2 r)(6) = r(5) and (DES-PC2 r)(7) = r(3) and (DES-PC2 r)(8) = r(28) and (DES-PC2 r)(9) = r(15) and (DES-PC2 r)(10) = r(6) and (DES-PC2 r)(11) = r(21) and (DES-PC2 r)(12) = r(10) and (DES-PC2 r)(13) = r(23) and (DES-PC2 r)(14) = r(19) and (DES-PC2 r)(15) = r(12) and (DES-PC2 r)(16) = r(4) and (DES-PC2 r)(17) = r(26) and (DES-PC2 r)(18) = r(8) and (DES-PC2 r)(19) = r(16) and (DES-PC2 r)(20) = r(7) and (DES-PC2 r)(21) = r(27) and (DES-PC2 r)(22) = r(20) and (DES-PC2 r)(23) = r(13) and (DES-PC2 r)(24) = r(2) and (DES-PC2 r)(25) = r(41) and (DES-PC2 r)(26) = r(52) and (DES-PC2 r)(27) = r(31) and (DES-PC2 r)(28) = r(37) and (DES-PC2 r)(29) = r(47) and (DES-PC2 r)(30) = r(55) and (DES-PC2 r)(31) = r(30) and (DES-PC2 r)(32) = r(40) and (DES-PC2 r)(33) = r(51) and (DES-PC2 r)(34) = r(45) and (DES-PC2 r)(35) = r(33) and (DES-PC2 r)(36) = r(48) and (DES-PC2 r)(37) = r(44) and (DES-PC2 r)(38) = r(49) and (DES-PC2 r)(39) = r(39) and (DES-PC2 r)(40) = r(56) and (DES-PC2 r)(41) = r(34) and (DES-PC2 r)(42) = r(53) and (DES-PC2 r)(43) = r(46) and (DES-PC2 r)(44) = r(42) and (DES-PC2 r)(45) = r(50) and (DES-PC2 r)(46) = r(36) and (DES-PC2 r)(47) = r(29) and

(DES-PC2 r)(48) $= r(32)$.

The finite sequence $\text{bitshift}_{\text{DES}}$ of elements of $\mathbb{N}$ is defined by the conditions (Def. 27).

(Def. 27) $\text{bitshift}_{\text{DES}}$ is 16-element and $(\text{bitshift}_{\text{DES}})(1) = 1$ and $(\text{bitshift}_{\text{DES}})(2) = 1$ and $(\text{bitshift}_{\text{DES}})(3) = 2$ and $(\text{bitshift}_{\text{DES}})(4) = 2$ and $(\text{bitshift}_{\text{DES}})(5) = 2$ and $(\text{bitshift}_{\text{DES}})(6) = 2$ and $(\text{bitshift}_{\text{DES}})(7) = 2$ and $(\text{bitshift}_{\text{DES}})(8) = 2$ and $(\text{bitshift}_{\text{DES}})(9) = 1$ and $(\text{bitshift}_{\text{DES}})(10) = 2$ and $(\text{bitshift}_{\text{DES}})(11) = 2$ and $(\text{bitshift}_{\text{DES}})(12) = 2$ and $(\text{bitshift}_{\text{DES}})(13) = 2$ and $(\text{bitshift}_{\text{DES}})(14) = 2$ and $(\text{bitshift}_{\text{DES}})(15) = 2$ and $(\text{bitshift}_{\text{DES}})(16) = 1$.

Let K_1 be an element of $\mathit{Boolean}^{64}$. The functor DES-KS K_1 yielding an element of $(\mathit{Boolean}^{48})^{16}$ is defined by the condition (Def. 28).

(Def. 28) There exist sequences C, D of $\mathit{Boolean}^{28}$ such that

- (i) $C(0) = \text{Op-Left}(\text{DES-PC1}\, K_1, 28)$,
- (ii) $D(0) = \text{Op-Right}(\text{DES-PC1}\, K_1, 28)$, and
- (iii) for every element i of $\mathbb{N}$ such that $0 \leq i \leq 15$ holds $(\text{DES-KS}\, K_1)(i + 1) = \text{DES-PC2}(C(i + 1) \frown D(i + 1))$ and $C(i + 1) = \text{Op-Shift}(C(i), (\text{bitshift}_{\text{DES}})(i))$ and $D(i + 1) = \text{Op-Shift}(D(i), (\text{bitshift}_{\text{DES}})(i))$.

6. Encryption and Decryption

Let n, m, k be non empty elements of $\mathbb{N}$, let R_1 be an element of $(\mathit{Boolean}^m)^k$, let F be a function from $\mathit{Boolean}^n \times \mathit{Boolean}^m$ into $\mathit{Boolean}^n$, let I_1 be a permutation of $\mathit{Boolean}^{2 \cdot n}$, and let M be an element of $\mathit{Boolean}^{2 \cdot n}$. The functor DES-like-CoDec(M, F, I_1, R_1) yields an element of $\mathit{Boolean}^{2 \cdot n}$ and is defined by the condition (Def. 29).

(Def. 29) There exist sequences L, R of $\mathit{Boolean}^n$ such that

- (i) $L(0) = \text{SP-Left}\, I_1(M)$,
- (ii) $R(0) = \text{SP-Right}\, I_1(M)$,
- (iii) for every element i of $\mathbb{N}$ such that $0 \leq i \leq k - 1$ holds $L(i + 1) = R(i)$ and $R(i + 1) = \text{Op-XOR}(L(i), F(R(i), (R_1)_{i+1}))$, and
- (iv) $\text{DES-like-CoDec}(M, F, I_1, R_1) = {I_1}^{-1}(R(k) \frown L(k))$.

The following proposition is true

(38) Let n, m, k be non empty elements of $\mathbb{N}$, R_1 be an element of $(\mathit{Boolean}^m)^k$, F be a function from $\mathit{Boolean}^n \times \mathit{Boolean}^m$ into $\mathit{Boolean}^n$, I_1 be a permutation of $\mathit{Boolean}^{2 \cdot n}$, and M be an element of $\mathit{Boolean}^{2 \cdot n}$. Then $\text{DES-like-CoDec}(\text{DES-like-CoDec}(M, F, I_1, R_1), F, I_1, \text{Rev}(R_1)) = M$.

Let R_1 be an element of $(\mathit{Boolean}^{48})^{16}$, let F be a function from $\mathit{Boolean}^{32} \times \mathit{Boolean}^{48}$ into $\mathit{Boolean}^{32}$, let I_1 be a permutation of $\mathit{Boolean}^{64}$, and let M be an element of $Boolean^{64}$. The functor DES-CoDec(M, F, I_1, R_1) yielding an element of $Boolean^{64}$ is defined by:

(Def. 30) There exists a permutation I_2 of $Boolean^{2 \cdot 32}$ and there exists an element M_1 of $Boolean^{2 \cdot 32}$ such that $I_2 = I_1$ and $M_1 = M$ and DES-CoDec$(M, F, I_1, R_1) =$ DES-like-CoDec(M_1, F, I_2, R_1).

The following proposition is true

(39) Let R_1 be an element of $(Boolean^{48})^{16}$, F be a function from $Boolean^{32} \times Boolean^{48}$ into $Boolean^{32}$, I_1 be a permutation of $Boolean^{64}$, and M be an element of $Boolean^{64}$.
Then DES-CoDec(DES-CoDec$(M, F, I_1, R_1), F, I_1, \mathrm{Rev}(R_1)) = M$.

Let p_1, s_9 be elements of $Boolean^{64}$. The functor DES-ENC(p_1, s_9) yields an element of $Boolean^{64}$ and is defined by:

(Def. 31) DES-ENC$(p_1, s_9) =$ DES-CoDec$(p_1$, DES-FFUNC, DES-PIP, DES-KS $s_9)$.

Let c_1, s_9 be elements of $Boolean^{64}$. The functor DES-DEC(c_1, s_9) yields an element of $Boolean^{64}$ and is defined as follows:

(Def. 32) DES-DEC$(c_1, s_9) =$
DES-CoDec$(c_1$, DES-FFUNC, DES-PIP, Rev(DES-KS $s_9))$.

The following proposition is true

(40) For all elements m_1, s_9 of $Boolean^{64}$ holds
DES-DEC(DES-ENC$(m_1, s_9), s_9) = m_1$.

REFERENCES

[1] Grzegorz Bancerek. Cardinal numbers. *Formalized Mathematics*, 1(**2**):377–382, 1990.
[2] Grzegorz Bancerek. The fundamental properties of natural numbers. *Formalized Mathematics*, 1(**1**):41–46, 1990.
[3] Grzegorz Bancerek. The ordinal numbers. *Formalized Mathematics*, 1(**1**):91–96, 1990.
[4] Grzegorz Bancerek and Krzysztof Hryniewiecki. Segments of natural numbers and finite sequences. *Formalized Mathematics*, 1(**1**):107–114, 1990.
[5] Czesław Byliński. Binary operations. *Formalized Mathematics*, 1(**1**):175–180, 1990.
[6] Czesław Byliński. Finite sequences and tuples of elements of a non-empty sets. *Formalized Mathematics*, 1(**3**):529–536, 1990.
[7] Czesław Byliński. Functions and their basic properties. *Formalized Mathematics*, 1(**1**):55–65, 1990.
[8] Czesław Byliński. Functions from a set to a set. *Formalized Mathematics*, 1(**1**):153–164, 1990.
[9] Czesław Byliński. Partial functions. *Formalized Mathematics*, 1(**2**):357–367, 1990.
[10] Czesław Byliński. Some basic properties of sets. *Formalized Mathematics*, 1(**1**):47–53, 1990.
[11] Czesław Byliński. Some properties of restrictions of finite sequences. *Formalized Mathematics*, 5(**2**):241–245, 1996.
[12] Shunichi Kobayashi and Kui Jia. A theory of Boolean valued functions and partitions. *Formalized Mathematics*, 7(**2**):249–254, 1998.
[13] Jarosław Kotowicz. Functions and finite sequences of real numbers. *Formalized Mathematics*, 3(**2**):275–278, 1992.
[14] Takaya Nishiyama and Yasuho Mizuhara. Binary arithmetics. *Formalized Mathematics*, 4(**1**):83–86, 1993.

[15] U.S. Department of Commerce/National Institute of Standards and Technology. Fips pub 46-3, data encryption standard (DES). `http://csrc.nist.gov/publications/fips/-fips46-3/fips46-3.pdf`. *Federal Information Processing Standars Publication*, 1999.
[16] Andrzej Trybulec. Domains and their Cartesian products. *Formalized Mathematics*, 1(**1**):115–122, 1990.
[17] Michał J. Trybulec. Integers. *Formalized Mathematics*, 1(**3**):501–505, 1990.
[18] Wojciech A. Trybulec. Pigeon hole principle. *Formalized Mathematics*, 1(**3**):575–579, 1990.
[19] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(**1**):67–71, 1990.
[20] Edmund Woronowicz. Many argument relations. *Formalized Mathematics*, 1(**4**):733–737, 1990.
[21] Edmund Woronowicz. Relations and their basic properties. *Formalized Mathematics*, 1(**1**):73–83, 1990.
[22] Edmund Woronowicz. Relations defined on sets. *Formalized Mathematics*, 1(**1**):181–186, 1990.

Received November 30, 2011