1.3 An example of a DES encryption

We here give an example showing how the encryption proceeds for a fixed key and a fixed plaintext. We encrypt the plaintext

0000000100100011010001010110011110001001101010111100110111101111

using the key (with parity check bits)

0001001**1**0011010**0**0101011**1**0111100**1**1001101**1**1011110**0**1101111**1**1111000**1**.

In hexadecimal notation this is written

Plaintext:	0123456789ABCDEF
Key:	133457799BBCDFF1

Applying IP we get L_0R_0 as

L_0R_0:	CC00CCFFF0AAF0AA

Then 16 rounds of encryption are performed, resulting in the following partial values.

K_1:	1B02EFFC7072	K_2:	79AED9DBC9E5
$E(R_0)$:	7A15557A1555	$E(R_1)$:	75EA5430AA09
$E(R_0) + K_0$:	6117BA866527	$E(R_1) + K_2$:	0C448DEB63EC
$f(R_0, K_1)$:	234AA9BB	$f(R_1, K_2)$:	3CAB87A3
L_1R_1:	F0AAF0AA - EF4A6544	L_2R_2:	EF4A6544 - CC017709
K_3:	55FC8A42CF99	K_4:	72ADD6DB351D
$E(R_2)$:	E58002BAE853	$E(R_3)$:	5042F8057FA9
$E(R_2) + K_3$:	B07C88F827CA	$E(R_3) + K_4$:	22EF2EDE4AB4
$f(R_2, K_3)$:	4D166EB0	$f(R_3, K_4)$:	BB23774C
L_3R_3:	C017709 - A25C0BF4	L_4R_4:	A25C0BF4 - 77220045
K_5:	7CEC07EB53A8	K_6:	63A53E507B2F
$E(R_4)$:	BAE90400020A	$E(R_5)$:	C5425FD0C1AF
$E(R_4) + K_5$:	C60503EB51A2	$E(R_5) + K_6$:	A6E76180BA80
$f(R_4, K_5)$:	2813ADC3	$f(R_5, K_6)$:	9E45CD2C
L_5R_5:	77220045 - 8A4FA637	L_6R_6:	8A4FA637 - E967CD69
K_7:	EC84B7F618BC	K_8:	F78A3AC13BFB
$E(R_6)$:	F52B0FE5AB53	$E(R_7)$:	00C2555F40A0
$E(R_6) + K_7$:	19AFB813B3EF	$E(R_7) + K_8$:	F7486F9E7B5B
$f(R_6, K_7)$:	8C051C27	$f(R_7, K_8)$:	3C0E86F9
L_7R_7:	E967CD69 - 064ABA10	L_8R_8:	064ABA10 - D5694B90
K_9:	E0DBEBEDE781	K_{10}:	B1F347BA464F
$E(R_8)$:	6AAB52A57CA1	$E(R_9)$:	1083F960C3F4
$E(R_8) + K_9$:	8A70B9489B20	$E(R_9) + K_{10}$:	A170BEDA85BB
$f(R_8, K_9)$:	22367C6A	$f(R_9, K_{10})$:	62BC9C22
L_9R_9:	D5694B90 - 247CC67A	$L_{10}R_{10}$:	247CC67A - B7D5D7B2
K_{11}:	215FD3DED386	K_{12}:	7571F59467E9
$E(R_{10})$:	5AFEABEAFDA5	$E(R_{11})$:	60ABF01F83F1
$E(R_{10}) + K_{11}$:	7BA178342E23	$E(R_{11}) + K_{12}$:	15DA058BE418
$f(R_{10}, K_{11})$:	E104FA02	$f(R_{11}, K_{12})$:	C268CFEA
$L_{11}R_{11}$:	B7D5D7B2 - C5783C78	$L_{12}R_{12}$:	C5783C78 - 75BD1858
K_{13}:	97C5D1FABA41	K_{14}:	5F43B7F2E73A
$E(R_{12})$:	3ABDFA8F02F0	$E(R_{13})$:	0F16068AAAF4
$E(R_{12}) + K_{13}$:	AD782B75B8B1	$E(R_{13}) + K_{14}$:	5055B1784DCE
$f(R_{12}, K_{13})$:	DDBB2922	$f(R_{13}, K_{14})$:	B7318E55
$L_{13}R_{13}$:	75BD1858 - 18C3155A	$L_{14}R_{14}$:	18C3155A - C28C960D
K_{15}:	BF918D3D3F0A	K_{16}:	CB3D8B0E17F5
$E(R_{14})$:	E054594AC05B	$E(R_{15})$:	206A041A41A8
$E(R_{14}) + K_{15}$:	5FC5D477FF51	$E(R_{15}) + K_{16}$:	EB578F14565D
$f(R_{14}K_{15})$:	5B81276E	$f(R_{15}, K_{16})$:	C8C04F98
$L_{15}R_{15}$:	C28C960D - 43423234	$L_{16}R_{16}$:	43423234 - 0A4CD995

Applying IP^{-1} to the reversed bitstring $R_{16}L_{16}$ we finally obtain the ciphertext as