| | |
|---|---|
| | **Initialization** |
| $\underline{k}$ | 0001 0011 0011 0100 0101 0011 0111 1001 1001 1011 1011 1100 1101 1111 1111 0001 |
| $\underline{c}_0\ \underline{d}_0$ | 1111000011001100101010101111 * 0101010101100010011110001111 |
| $\underline{x}$ | 01010101 01010101 01010101 01010101 01010101 01010101 01010101 01010101 |
| IP$[\underline{x}]$ | 11111111 11111111 11111111 11111111 00000000 00000000 00000000 00000000 |
| $(L[0], R[0])$ | 11111111 11111111 11111111 11111111 * 00000000 00000000 00000000 00000000 |
| | **Round 1** |
| $(L[0], R[0])$ | 11111111 11111111 11111111 11111111 * 00000000 00000000 00000000 00000000 |
| $\underline{c}_0\ \underline{d}_0$ | 1111000011001100101010101111 * 0101010101100010011110001111 |
| $\underline{c}_1\ \underline{d}_1$ | 1110000110011001010101011111 * 1010101011000100111100011110 |
| KEY[1] | 000110 110000 001011 101111 011111 000111 000001 110010 |
| $E[R[0]]$ | 000000 000000 000000 000000 000000 000000 000000 000000 |
| $E[R[0]] + KEY[1]$ | 000110 110000 001011 101111 011111 000111 000001 110010 |
| $SBOX$ | 0001 0101 0100 1000 0110 0010 1101 0110 |
| $PBOX$ | 0000 0010 0011 0111 0100 0000 1111 0011 |
| $L[0]$ | 1111 1111 1111 1111 1111 1111 1111 1111 |
| $PBOX + L[0]$ | 1111 1101 1100 1000 1011 1111 0000 1100 |
| $(PBOX + L[0], R[0])$ | 11111101 11001000 10111111 00001100 * 00000000 00000000 00000000 00000000 |
| $(L[1], R[1])$ | 00000000 00000000 00000000 00000000 * 11111101 11001000 10111111 00001100 |
| | **Round 2** |
| $(L[1], R[1])$ | 00000000 00000000 00000000 00000000 * 11111101 11001000 10111111 00001100 |
| $\underline{c}_1\ \underline{d}_1$ | 1110000110011001010101011111 * 1010101011000100111100011110 |
| $\underline{c}_2\ \underline{d}_2$ | 1100001100110010101010111111 * 0101010110001001111000111101 |
| KEY[2] | 011110 011010 111011 011001 110110 101100 100111 100101 |
| $E[R[1]]$ | 011111 111011 111001 010001 010111 111110 100001 011001 |
| $E[R[1]] + KEY[2]$ | 000001 100001 000010 001000 100001 010010 000110 111100 |
| $SBOX$ | 0000 1101 0000 0000 1011 1101 1110 0101 |
| $PBOX$ | 0011 0001 0001 1000 0110 1100 1011 1001 |
| $L[1]$ | 0000 0000 0000 0000 0000 0000 0000 0000 |
| $PBOX + L[1]$ | 0011 0001 0001 1000 0110 1100 1011 1001 |
| $(PBOX + L[1], R[1])$ | 00110001 00011000 01101100 10111001 * 11111101 11001000 10111111 00001100 |
| $(L[2], R[2])$ | 11111101 11001000 10111111 00001100 * 00110001 00011000 01101100 10111001 |
| | **Round 3** |
| $(L[2], R[2])$ | 11111101 11001000 10111111 00001100 * 00110001 00011000 01101100 10111001 |
| $\underline{c}_2\ \underline{d}_2$ | 1100001100110010101010111111 * 0101010110001001111000111101 |
| $\underline{c}_3\ \underline{d}_3$ | 0000110011001010101011111111 * 0101011000100111100011110101 |
| KEY[3] | 010101 011111 110010 001010 010000 101100 111110 011001 |
| $E[R[2]]$ | 100110 100010 100011 110000 001101 011001 010111 110010 |
| $E[R[2]] + KEY[3]$ | 110011 111101 010001 111010 011101 110101 101001 101011 |
| $SBOX$ | 1011 1110 0010 0010 1000 0001 0001 1010 |
| $PBOX$ | 0100 1011 1100 1010 0010 0010 0001 0110 |
| $L[2]$ | 1111 1101 1100 1000 1011 1111 0000 1100 |
| $PBOX + L[2]$ | 1011 0110 0000 0010 1001 1101 0001 1010 |
| $(PBOX + L[2], R[2])$ | 10110110 00000010 10011101 00011010 * 00110001 00011000 01101100 10111001 |
| $(L[3], R[3])$ | 00110001 00011000 01101100 10111001 * 10110110 00000010 10011101 00011010 |

**Round 4**

| | |
|---|---|
| $(L[3], R[3])$ | 00110001 00011000 01101100 10111001 * 10110110 00000010 10011101 00011010 |
| $\underline{c}_3\ \underline{d}_3$ | 00001100110010101010111111111 * 01010110001001111000111101 01 |
| $\underline{c}_4\ \underline{d}_4$ | 00110011001010101011111111100 * 01011000100111100011110101 01 |
| KEY[4] | 011100 101010 110111 010110 110110 110011 010100 011001 |
| $E[R[3]]$ | 010110 101100 000000 000101 010011 111010 100011 110101 |
| $E[R[3]] + KEY[4]$ | 001010 000110 110111 010011 100101 001001 110111 101100 |
| $SBOX$ | 1111 1110 0011 0111 1100 0111 1111 1110 |
| $PBOX$ | 1100 1111 1111 1110 1011 0110 0011 1111 |
| $L[3]$ | 0011 0001 0001 1000 0110 1100 1011 1001 |
| $PBOX + L[3]$ | 1111 1110 1110 0110 1101 1010 1000 0110 |
| $(PBOX + L[3], R[3])$ | 11111110 11100110 11011010 10000110 * 10110110 00000010 10011101 00011010 |
| $(L[4], R[4])$ | 10110110 00000010 10011101 00011010 * 11111110 11100110 11011010 10000110 |

**Round 5**

| | |
|---|---|
| $(L[4], R[4])$ | 10110110 00000010 10011101 00011010 * 11111110 11100110 11011010 10000110 |
| $\underline{c}_4\ \underline{d}_4$ | 00110011001010101011111111100 * 01011000100111100011110101 01 |
| $\underline{c}_5\ \underline{d}_5$ | 11001100101010101111111110000 * 01100010011110001111010101 01 |
| KEY[5] | 011111 001110 110000 000111 111010 110101 001100 101000 |
| $E[R[4]]$ | 011111 111101 011100 001101 011011 110101 010000 001101 |
| $E[R[4]] + KEY[5]$ | 000000 110011 101100 001010 100001 000000 011100 100101 |
| $SBOX$ | 1110 0110 0011 0110 1011 1100 0110 1110 |
| $PBOX$ | 0111 1101 1101 0010 1001 0110 1011 1100 |
| $L[4]$ | 1011 0110 0000 0010 1001 1101 0001 1010 |
| $PBOX + L[4]$ | 1100 1011 1101 0000 0000 1011 1010 0110 |
| $(PBOX + L[4], R[4])$ | 11001011 11010000 00001011 10100110 * 11111110 11100110 11011010 10000110 |
| $(L[5], R[5])$ | 11111110 11100110 11011010 10000110 * 11001011 11010000 00001011 10100110 |

**Round 6**

| | |
|---|---|
| $(L[5], R[5])$ | 11111110 11100110 11011010 10000110 * 11001011 11010000 00001011 10100110 |
| $\underline{c}_5\ \underline{d}_5$ | 11001100101010101111111110000 * 01100010011110001111010101 01 |
| $\underline{c}_6\ \underline{d}_6$ | 00110010101010111111111000011 * 10001001111000111101010101 01 |
| KEY[6] | 011000 111010 010100 111110 010100 000111 101100 101110 |
| $E[R[5]]$ | 011001 010111 111010 100000 000001 010111 110100 001101 |
| $E[R[5]] + KEY[6]$ | 000001 101101 101110 011110 010101 010000 011000 100011 |
| $SBOX$ | 0000 0100 0000 1111 1111 0000 0101 0001 |
| $PBOX$ | 1010 0011 0101 0100 0001 1000 1101 0000 |
| $L[5]$ | 1111 1110 1110 0110 1101 1010 1000 0110 |
| $PBOX + L[5]$ | 0101 1101 1011 0010 1100 0010 0101 0110 |
| $(PBOX + L[5], R[5])$ | 01011101 10110010 11000010 01010110 * 11001011 11010000 00001011 10100110 |
| $(L[6], R[6])$ | 11001011 11010000 00001011 10100110 * 01011101 10110010 11000010 01010110 |

| | |
|---|---|
| | **Round 7** |
| $(L[6], R[6])$ | 11001011 11010000 00001011 10100110 * 01011101 10110010 11000010 01010110 |
| $\underline{c}_6\ \underline{d}_6$ | 00110010101010111111111000011 * 10001001111000111101010101010 |
| $\underline{c}_7\ \underline{d}_7$ | 11001010101011111111100001100 * 00100111100011111010101010110 |
| KEY[7] | 111011 001000 010010 110111 111101 000001 100010 111100 |
| $E[R[6]]$ | 001011 111011 110110 100101 011000 000100 001010 101100 |
| $E[R[6]] + KEY[7]$ | 110000 110011 100100 010010 100101 000101 101000 010000 |
| $SBOX$ | 1111 0110 0100 0010 1100 0100 1100 1010 |
| $PBOX$ | 0100 1001 1101 0111 1000 0010 0001 1011 |
| $L[6]$ | 1100 1011 1101 0000 0000 1011 1010 0110 |
| $PBOX + L[6]$ | 1000 0010 0000 0111 1000 1001 1011 1101 |
| $(PBOX + L[6], R[6])$ | 10000010 00000111 10001001 10111101 * 01011101 10110010 11000010 01010110 |
| $(L[7], R[7])$ | 01011101 10110010 11000010 01010110 * 10000010 00000111 10001001 10111101 |
| | **Round 8** |
| $(L[7], R[7])$ | 01011101 10110010 11000010 01010110 * 10000010 00000111 10001001 10111101 |
| $\underline{c}_7\ \underline{d}_7$ | 11001010101011111111100001100 * 00100111100011111010101010110 |
| $\underline{c}_8\ \underline{d}_8$ | 00101010101111111110000110011 * 10011110001111010101011000 |
| KEY[8] | 111101 111000 101000 111010 110000 010011 101011 111011 |
| $E[R[7]]$ | 110000 000100 000000 001111 110001 010011 110111 111011 |
| $E[R[7]] + KEY[8]$ | 001101 111100 101000 110101 000001 000000 011100 000000 |
| $SBOX$ | 1101 0010 1000 0101 1110 1100 0110 1101 |
| $PBOX$ | 1101 1001 1001 0100 1001 1101 1010 1010 |
| $L[7]$ | 0101 1101 1011 0010 1100 0010 0101 0110 |
| $PBOX + L[7]$ | 1000 0100 0010 0110 0101 1111 1111 1100 |
| $(PBOX + L[7], R[7])$ | 10000100 00100110 01011111 11111100 * 10000010 00000111 10001001 10111101 |
| $(L[8], R[8])$ | 10000010 00000111 10001001 10111101 * 10000100 00100110 01011111 11111100 |
| | **Round 9** |
| $(L[8], R[8])$ | 10000010 00000111 10001001 10111101 * 10000100 00100110 01011111 11111100 |
| $\underline{c}_8\ \underline{d}_8$ | 00101010101111111110000110011 * 10011110001111010101011000 |
| $\underline{c}_9\ \underline{d}_9$ | 01010101011111111100001100110 * 00111100011110101010110001 |
| KEY[9] | 111000 001101 101111 101011 111010 011110 011110 000001 |
| $E[R[8]]$ | 010000 001000 000100 001100 001011 111111 111111 111001 |
| $E[R[8]] + KEY[9]$ | 101000 000101 101011 100111 110001 100001 100001 111000 |
| $SBOX$ | 1101 0100 1001 0110 0110 0100 0110 1111 |
| $PBOX$ | 0000 1100 1101 0110 1001 1101 1011 1010 |
| $L[8]$ | 1000 0010 0000 0111 1000 1001 1011 1101 |
| $PBOX + L[8]$ | 1000 1110 1101 0001 0001 0100 0000 0111 |
| $(PBOX + L[8], R[8])$ | 10001110 11010001 00010100 00000111 * 10000100 00100110 01011111 11111100 |
| $(L[9], R[9])$ | 10000100 00100110 01011111 11111100 * 10001110 11010001 00010100 00000111 |

| | |
|---|---|
| | **Round 10** |
| $(L[9], R[9])$ | 10000100 00100110 01011111 11111100 * 10001110 11010001 00010100 00000111 |
| $\underline{c}_9\ \underline{d}_9$ | 0101010101111111100001100110 * 0011110001111010101010110001 |
| $\underline{c}_{10}\ \underline{d}_{10}$ | 0101010111111111000011001 1 * 1111000111101010101011000100 |
| KEY[10] | 101100 011111 001101 000111 101110 100100 011000 001111 |
| $E[R[9]]$ | 110001 011101 011010 100010 100010 101000 000000 001111 |
| $E[R[9]] + KEY[10]$ | 011101 000010 010111 100101 001100 001100 011000 000000 |
| $SBOX$ | 0011 0001 1110 0000 1011 0110 0101 1101 |
| $PBOX$ | 0010 1011 0011 0001 0100 1011 1010 1110 |
| $L[9]$ | 1000 0100 0010 0110 0101 1111 1111 1100 |
| $PBOX + L[9]$ | 1010 1111 0001 0111 0001 0100 0101 0010 |
| $(PBOX + L[9], R[9])$ | 10101111 00010111 00010100 01010010 * 10001110 11010001 00010100 00000111 |
| $(L[10], R[10])$ | 10001110 11010001 00010100 00000111 * 10101111 00010111 00010100 01010010 |
| | **Round 11** |
| $(L[10], R[10])$ | 10001110 11010001 00010100 00000111 * 10101111 00010111 00010100 01010010 |
| $\underline{c}_{10}\ \underline{d}_{10}$ | 0101010111111111000011001 1 * 1111000111101010101011000100 |
| $\underline{c}11\ \underline{d}11$ | 0101011111111100001100110 0101 * 1100011110101010101100010011 |
| KEY[11] | 001000 010101 111111 010011 110111 100101 001110 000110 |
| $E[R[10]]$ | 010101 011110 100010 101110 100010 101000 001010 100101 |
| $E[R[10]] + KEY[11]$ | 011101 001011 011101 111101 010101 001101 000100 100011 |
| $SBOX$ | 0011 0010 1111 0010 1111 1001 0010 0001 |
| $PBOX$ | 0111 0101 0100 0101 0010 1111 1000 0110 |
| $L[10]$ | 1000 1110 1101 0001 0001 0100 0000 0111 |
| $PBOX + L[10]$ | 1111 1011 1001 0100 0011 1011 1000 0001 |
| $(PBOX + L[10], R[10])$ | 11111011 10010100 00111011 10000001 * 10101111 00010111 00010100 01010010 |
| $(L[11], R[11])$ | 10101111 00010111 00010100 01010010 * 11111011 10010100 00111011 10000001 |
| | **Round 12** |
| $(L[11], R[11])$ | 10101111 00010111 00010100 01010010 * 11111011 10010100 00111011 10000001 |
| $\underline{c}_{11}\ \underline{d}_{11}$ | 0101011111111100001100110 0101 * 1100011110101010101100010011 |
| $\underline{c}_{12}\ \underline{d}_{12}$ | 0101111111100001100110010101 * 0001111010101010110001001111 |
| KEY[12] | 011101 010111 000111 110101 100101 000110 001111 101001 |
| $E[R[11]]$ | 111111 110111 110010 101000 000111 110111 110000 000011 |
| $E[R[11]] + KEY[12]$ | 100010 100000 110101 011101 100010 110001 111111 101010 |
| $SBOX$ | 0001 0000 1110 1110 0010 1011 1100 1100 |
| $PBOX$ | 0001 1000 0111 0001 0011 0001 1110 0111 |
| $L[11]$ | 1010 1111 0001 0111 0001 0100 0101 0010 |
| $PBOX + L[11]$ | 1011 0111 0110 0110 0010 0101 1011 0101 |
| $(PBOX + L[11], R[11])$ | 10110111 01100110 00100101 10110101 * 11111011 10010100 00111011 10000001 |
| $(L[12], R[12])$ | 11111011 10010100 00111011 10000001 * 10110111 01100110 00100101 10110101 |

| | **Round 13** |
|---|---|
| $(L[12], R[12])$ | 11111011 10010100 00111011 10000001 * 10110111 01100110 00100101 10110101 |
| $\underline{c}_{12}\ \underline{d}_{12}$ | 0101111111100001100110010101 * 000111101010101010110001001111 |
| $\underline{c}_{13}\ \underline{d}_{13}$ | 0111111110000110011001010101 * 011110101010101011000100111100 |
| KEY[13] | 100101 111100 010111 010001 111100 101011 101001 000001 |
| $E[R[12]]$ | 110110 101110 101100 001100 000100 001011 110110 101011 |
| $E[R[12]] + KEY[13]$ | 010011 010010 111011 011101 111000 100000 011111 101010 |
| $SBOX$ | 0110 0111 0101 1110 0110 1001 0110 1100 |
| $PBOX$ | 0101 1100 0101 0101 1111 0110 1111 0000 |
| $L[12]$ | 1111 1011 1001 0100 0011 1011 1000 0001 |
| $PBOX + L[12]$ | 1010 0111 1100 0001 1100 1101 0111 0001 |
| $(PBOX + L[12], R[12])$ | 10100111 11000001 11001101 01110001 * 10110111 01100110 00100101 10110101 |
| $(L[13], R[13])$ | 10110111 01100110 00100101 10110101 * 10100111 11000001 11001101 01110001 |

| | **Round 14** |
|---|---|
| $(L[13], R[13])$ | 10110111 01100110 00100101 10110101 * 10100111 11000001 11001101 01110001 |
| $\underline{c}_{13}\ \underline{d}_{13}$ | 0111111110000110011001010101 * 011110101010101011000100111100 |
| $\underline{c}_{14}\ \underline{d}_{14}$ | 1111111000011001100101010101 * 111010101010110001001111000 1 |
| KEY[14] | 010111 110100 001110 110111 111100 101010 011100 111010 |
| $E[R[13]]$ | 110100 001111 111000 000011 111001 011010 101110 100011 |
| $E[R[13]] + KEY[14]$ | 100011 111011 110110 110100 000101 110000 110010 011001 |
| $SBOX$ | 1100 0101 1100 0011 0010 0111 1111 0000 |
| $PBOX$ | 1000 0010 1111 0001 1110 0101 1001 1001 |
| $L[13]$ | 1011 0111 0110 0110 0010 0101 1011 0101 |
| $PBOX + L[13]$ | 0011 0101 1001 0111 1100 0000 0010 1100 |
| $(PBOX + L[13], R[13])$ | 00110101 10010111 11000000 00101100 * 10100111 11000001 11001101 01110001 |
| $(L[14], R[14])$ | 10100111 11000001 11001101 01110001 * 00110101 10010111 11000000 00101100 |

| | **Round 15** |
|---|---|
| $(L[14], R[14])$ | 10100111 11000001 11001101 01110001 * 00110101 10010111 11000000 00101100 |
| $\underline{c}_{14}\ \underline{d}_{14}$ | 1111111000011001100101010101 * 111010101010110001001111000 1 |
| $\underline{c}_{15}\ \underline{d}_{15}$ | 1111100001100110010101010111 * 101010101011000100111100 0111 |
| KEY[15] | 101111 111001 000110 001101 001111 010011 111100 001010 |
| $E[R[14]]$ | 000110 101011 110010 101111 111000 000000 000101 011000 |
| $E[R[14]] + KEY[15]$ | 101001 010010 110100 100010 110111 010011 111001 010010 |
| $SBOX$ | 0100 0111 0010 0110 1001 0001 1110 1001 |
| $PBOX$ | 0110 1001 0101 0000 1111 1100 0001 0101 |
| $L[14]$ | 1010 0111 1100 0001 1100 1101 0111 0001 |
| $PBOX + L[14]$ | 1100 1110 1001 0001 0011 0001 0110 0100 |
| $(PBOX + L[14], R[14])$ | 11001110 10010001 00110001 01100100 * 00110101 10010111 11000000 00101100 |
| $(L[15], R[15])$ | 00110101 10010111 11000000 00101100 * 11001110 10010001 00110001 01100100 |

| | **Round 16** |
|---|---|
| $(L[15], R[15])$ | 00110101 10010111 11000000 00101100 * 11001110 10010001 00110001 01100100 |
| $\underline{c}_{15}\ \underline{d}_{15}$ | 11111000011001100101010101111 * 10101010101100010011111000111 |
| $\underline{c}_{16}\ \underline{d}_{16}$ | 11110000110011001010101011111 * 01010101011000100111100011111 |
| KEY[16] | 110010 110011 110110 001011 000011 100001 011111 100101 |
| $E[R[15]]$ | 011001 011101 010010 100010 100110 100010 101100 001001 |
| $E[R[15]] + KEY[16]$ | 101011 101110 100100 101001 100101 000011 110011 101100 |
| $SBOX$ | 1001 0001 0100 1010 1100 1111 0101 1110 |
| $PBOX$ | 0001 1011 1111 0111 0110 0000 0110 1010 |
| $L[15]$ | 0011 0101 1001 0111 1100 0000 0010 1100 |
| $PBOX + L[15]$ | 0010 1110 0110 0000 1010 0000 0100 0110 |
| $(PBOX + L[15], R[15])$ | 00101110 01100000 10100000 01000110 * 11001110 10010001 00110001 01100100 |
| $(L[16], R[16])$ | 00101110 01100000 10100000 01000110 * 11001110 10010001 00110001 01100100 |

| | **Output** |
|---|---|
| $\underline{y}$ | 00101000 11000001 11000011 11000000 00101000 01011110 10010011 10100100 |