Дослідимо **лавиновий ефект**. Розглянемо шифрування двох 64-бітних блоків, що відрізняються лише в 1 біті, однаковим ключем *К* = 13 34 57 79 9B BC DF F1

*К* = 0001001100110100010101110111100110011011101111001101111111110001

|  |  |  |  |
| --- | --- | --- | --- |
| *Raund* | Input block 1: 01 23 45 67 89 AB CD EF | Input block 2: 0**0** 23 45 67 89 AB CD EF | Δ (bits) |
| *IP* | L0: 11001100000000001100110011111111  R0: 11110000101010101111000010101010 | L0: 1100110000000000110011001111111**0**  R0: 11110000101010101111000010101010 | 1 |
| 1 | L1: 11110000101010101111000010101010  R1: 11101111010010100110010101000100 | L1: 11110000101010101111000010101010  R1: 1110111101001010011001010100010**1** | 1 |
| 2 | L2: 11101111010010100110010101000100  R2: 11001100000000010111011100001001 | L2: 1110111101001010011001010100010**1**  R2: 1100**0**10000000001011101**0**100**1**010**1**1 | 5 |
| 3 | L3: 11001100000000010111011100001001  R3: 10100010010111000000101111110100 | L3: 1100**0**10000000001011101**0**100**1**010**1**1  R3: 101**11**0**0**001**1**1**0**1**1**00**1**0010**0**111**001**1**1**0 | 16 |
| 4 | L4: 10100010010111000000101111110100  R4: 01110111001000100000000001000101 | L4: 101**11**0**0**001**1**1**0**1**1**00**1**0010**0**111**001**1**1**0  R4: **1**111**1000**0**10**000**01**0**1**0**11**0**1**0**10**00**1**1**10** | 30 |

Отже, при зміні лише одного біта у вхідному блоці після 4 раундів шифрування результат відрізняється в 30 бітах, тобто приблизно в половині бітів.