

* **Tìm khóa con: (64 bit)**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **hex** | d | a | 0 | 2 | c | e | 3 | a | 8 |
| **bin** | 1101 | 1010 | 0000 | 0010 | 1100 | 1110 | 0011 | 1010 | 1000 |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 9 | e | c | a | c | 3 | b |
| 1001 | 1110 | 1100 | 1010 | 1100 | 0011 | 1011 |

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| input | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
| key | 1 | 1 | 0 | 1 | 1 | 0 | 1 | 0 | 0 |

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 |
| 0 | 0 | 0 | 0 | 0 | 1 | 0 | 1 | 1 | 0 |

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 |
| 0 | 1 | 1 | 1 | 0 | 0 | 0 | 1 | 1 | 1 |

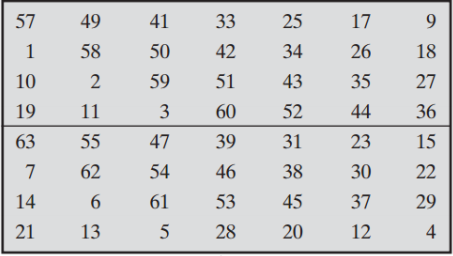
|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 30 | 31 | 32 | 33 | 34 | 35 | 36 | 37 | 38 | 39 |
| 0 | 1 | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 0 |

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 40 | 41 | 42 | 43 | 44 | 45 | 46 | 47 | 48 | 49 |
| 1 | 1 | 1 | 1 | 0 | 1 | 1 | 0 | 0 | 1 |

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 50 | 51 | 52 | 53 | 54 | 55 | 56 | 57 | 58 | 59 |
| 0 | 1 | 0 | 1 | 1 | 0 | 0 | 0 | 0 | 1 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 60 | 61 | 62 | 63 | 64 |
| 1 | 1 | 0 | 1 | 1 |

**+ Permuted Choice One (PC-1) (56 bit)**

****

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **pc1** | 57 | 49 | 41 | 33 | 25 | 17 | 9 | 1 | 58 |
| **value** | 0 | 1 | 1 | 1 | 0 | 1 | 0 | 1 | 0 |

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 50 | 42 | 34 | 26 | 18 | 10 | 2 | 59 | 51 | 43 |
| 0 | 1 | 0 | 0 | 1 | 0 | 1 | 1 | 1 | 1 |

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 35 | 27 | 19 | 11 | 3 | 60 | 52 | 44 | 36 | 63 |
| 0 | 1 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 1 |

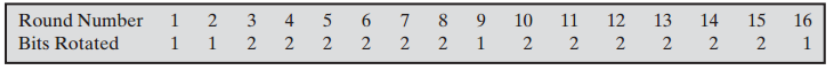
|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 55 | 47 | 39 | 31 | 23 | 15 | 7 | 62 | 54 | 46 |
| 0 | 0 | 0 | 1 | 1 | 1 | 1 | 0 | 1 | 1 |

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 38 | 30 | 22 | 14 | 6 | 61 | 53 | 45 | 37 | 29 |
| 0 | 0 | 1 | 0 | 0 | 1 | 1 | 1 | 1 | 1 |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 21 | 13 | 5 | 28 | 20 | 12 | 4 |
| 1 | 0 | 1 | 1 | 0 | 0 | 1 |

* **After PC1** = 0111 0101 0010 0101 1110 1000 1000 || 1000 1111 0110 0100 1111 1101 1001

**+ Left shift**

****

**Left shift 32 bit left =** 1110 1010 0100 1011 1101 0001 0000

**Left shift 32 bit right =** 0001 1110 1100 1001 1111 1011 0011

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| input | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
| key | 1 | 1 | 1 | 0 | 1 | 0 | 1 | 0 | 0 |

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 |
| 1 | 0 | 0 | 1 | 0 | 1 | 1 | 1 | 1 | 0 |

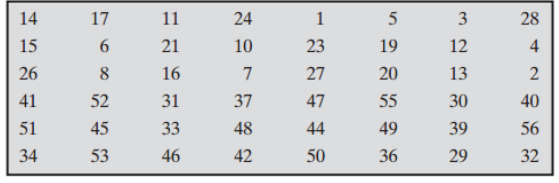
|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 |
| 1 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 |

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 30 | 31 | 32 | 33 | 34 | 35 | 36 | 37 | 38 | 39 |
| 0 | 0 | 1 | 1 | 1 | 1 | 0 | 1 | 1 | 0 |

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 40 | 41 | 42 | 43 | 44 | 45 | 46 | 47 | 48 | 49 |
| 0 | 1 | 0 | 0 | 1 | 1 | 1 | 1 | 1 | 1 |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 50 | 51 | 52 | 53 | 54 | 55 | 56 |
| 0 | 1 | 1 | 0 | 0 | 1 | 1 |

**+ Permuted choice 2 (48 bit)**

****

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **pc2** | 14 | 17 | 11 | 24 | 1 | 5 | 3 | 28 | 15 |
| **value** | 0 | 1 | 0 | 1 | 1 | 1 | 1 | 0 | 1 |

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 6 | 21 | 10 | 23 | 19 | 12 | 4 | 26 | 8 | 16 |
| 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 1 |

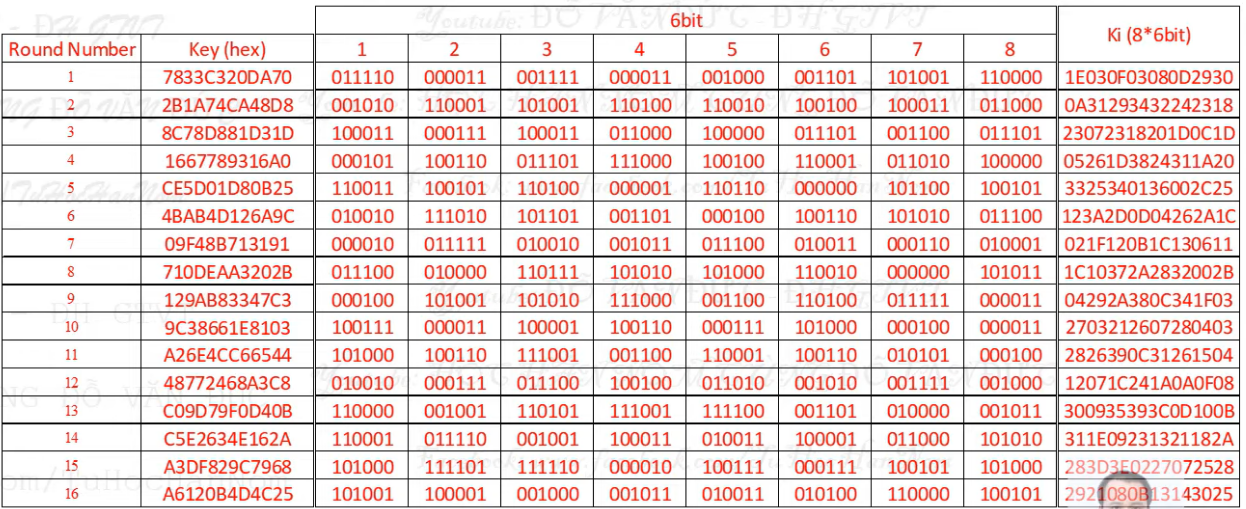
|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 7 | 27 | 20 | 13 | 2 | 41 | 52 | 31 | 37 | 47 |
| 1 | 0 | 1 | 1 | 1 | 1 | 1 | 0 | 1 | 1 |

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 55 | 30 | 40 | 51 | 45 | 33 | 48 | 44 | 49 | 39 |
| 1 | 0 | 0 | 1 | 1 | 1 | 1 | 1 | 1 | 0 |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 56 | 34 | 53 | 46 | 42 | 50 | 36 | 29 | 32 |
| 1 | 1 | 0 | 1 | 0 | 0 | 0 | 0 | 1 |

* **After PC2 =Key 1=** 0101 1110 1001 0000 0011 0111 1101 1100 1111 1101 1010 0001 = 5

**+ Tóm tắt khóa của 16 vòng lặp**

****

* **Mã hóa: (64 bit)**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **hex** | 0 | 2 | 4 | 6 | 8 | a | c | e | e |
| **bin** | 0000 | 0010 | 0100 | 0110 | 1000 | 1010 | 1100 | 1110 | 1100 |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| c | a | 8 | 6 | 4 | 2 | 0 |
| 1100 | 1010 | 1000 | 0110 | 0100 | 0010 | 0000 |

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **input** | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
| **key** | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 |

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 |
| 1 | 0 | 0 | 0 | 1 | 1 | 0 | 1 | 0 | 0 |

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 |
| 0 | 1 | 0 | 1 | 0 | 1 | 1 | 0 | 0 | 1 |

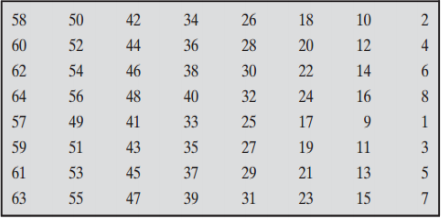
|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 30 | 31 | 32 | 33 | 34 | 35 | 36 | 37 | 38 | 39 |
| 1 | 1 | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 0 |

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 40 | 41 | 42 | 43 | 44 | 45 | 46 | 47 | 48 | 49 |
| 0 | 1 | 0 | 1 | 0 | 1 | 0 | 0 | 0 | 0 |

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 50 | 51 | 52 | 53 | 54 | 55 | 56 | 57 | 58 | 59 |
| 1 | 1 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 1 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 60 | 61 | 62 | 63 | 64 |
| 0 | 0 | 0 | 0 | 0 |

**+ Initial Permutation : IP(64 bit)**

****

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **IP** | 58 | 50 | 42 | 34 | 26 | 18 | 10 | 2 | 60 |
| **value** | 0 | 1 | 0 | 1 | 1 | 0 | 1 | 0 | 0 |

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 52 | 44 | 36 | 28 | 20 | 12 | 4 | 62 | 54 | 46 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 |

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 38 | 30 | 22 | 14 | 6 | 64 | 56 | 48 | 40 | 32 |
| 1 | 1 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 |

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 24 | 16 | 8 | 57 | 49 | 41 | 33 | 25 | 17 | 9 |
| 0 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 0 |

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | 59 | 51 | 43 | 35 | 27 | 19 | 11 | 3 | 61 |
| 0 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 |

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 53 | 45 | 37 | 29 | 21 | 13 | 5 | 63 | 55 | 47 |
| 0 | 1 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 0 |

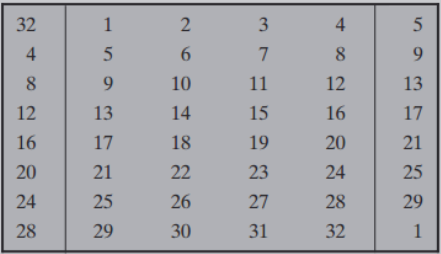
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 39 | 31 | 23 | 15 | 7 |
| 0 | 1 | 1 | 1 | 1 |

* **After IP =** 0101 1010 0000 0000 0101 1010 0000 0000 || 0011 1100 1110 0000 0011 1100 0000 1111

**L-left =** 0101 1010 0000 0000 0101 1010 0000 0000 (32 bit)

**L-right =** 0011 1100 1110 0000 0011 1100 0000 1111 (32 bit)

**+ Expansion/permutation (48 bit):**

****

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **input** | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
| **key** | 0 | 0 | 1 | 1 | 1 | 1 | 0 | 0 | 1 |

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 |
| 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 |

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 |
| 1 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 1 |

|  |  |  |
| --- | --- | --- |
| 30 | 31 | 32 |
| 1 | 1 | 1 |

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **E** | 32 | 1 | 2 | 3 | 4 | 5 | 4 | 5 | 6 |
| **value** | 1 | 0 | 0 | 1 | 1 | 1 | 1 | 1 | 1 |

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 7 | 8 | 9 | 8 | 9 | 10 | 11 | 12 | 13 | 12 |
| 0 | 0 | 1 | 0 | 1 | 1 | 1 | 0 | 0 | 0 |

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 13 | 14 | 15 | 16 | 17 | 16 | 17 | 18 | 19 | 20 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 |

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 21 | 20 | 21 | 22 | 23 | 24 | 25 | 24 | 25 | 26 |
| 1 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 27 | 28 | 29 | 28 | 29 | 30 | 31 | 32 | 1 |
| 0 | 0 | 1 | 0 | 1 | 1 | 1 | 1 | 0 |

* **After E =** 1001 1111 1001 0111 0000 0000 0001 1111 1000 0000 0101 1110

**+ Value E** XOR **Key 1: (48 bit)**

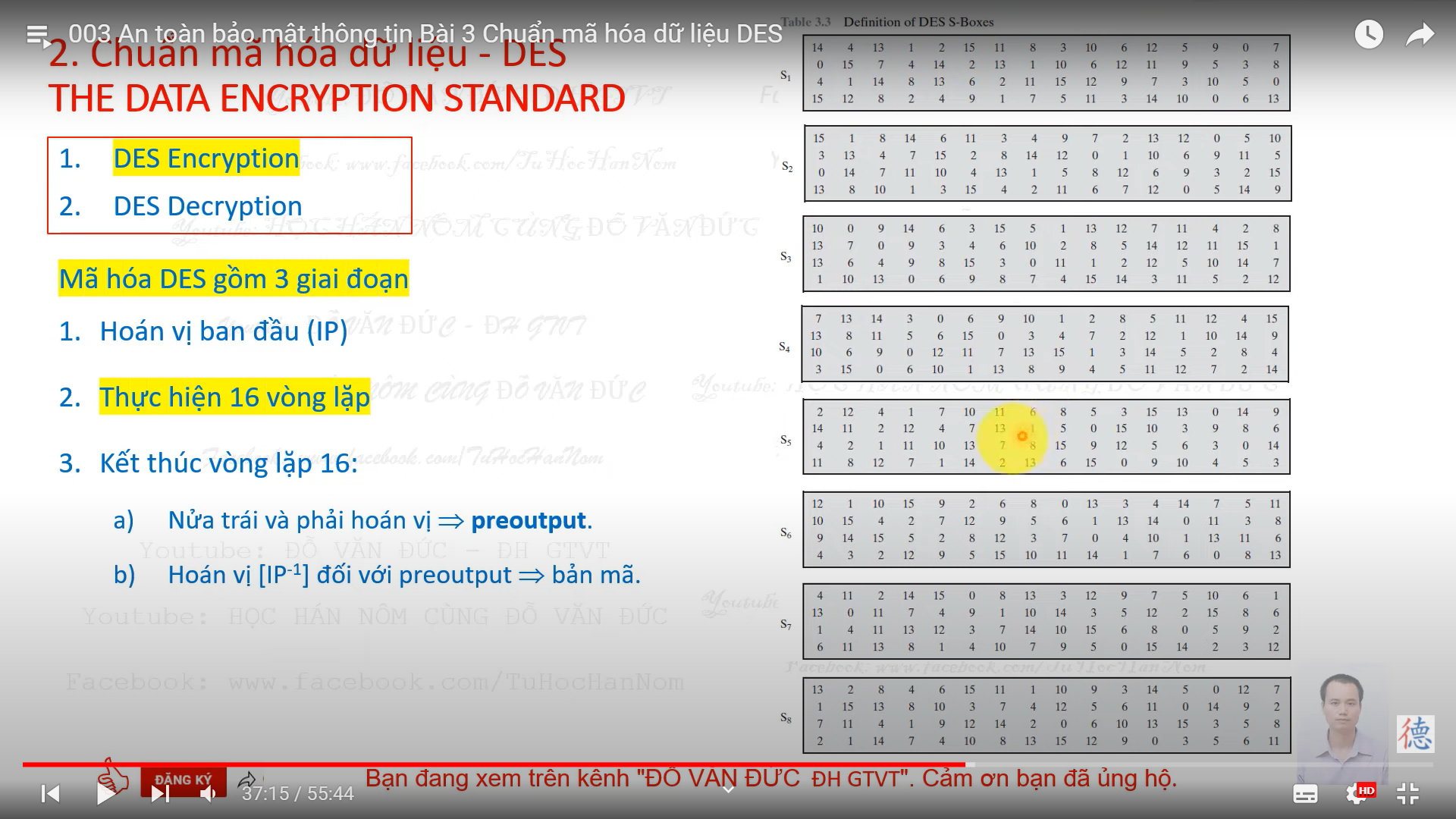
**Value E =** 1001 1111 1001 0111 0000 0000 0001 1111 1000 0000 0101 1110

**Key 1 =** 0111 1000 0011 0011 1100 0011 0010 0000 1101 1010 0111 0000

* **Result** = 1110 0111 1010 0100 1100 0011 0011 1111 0101 1010 0010 1110

**+ S box (32 bit)**

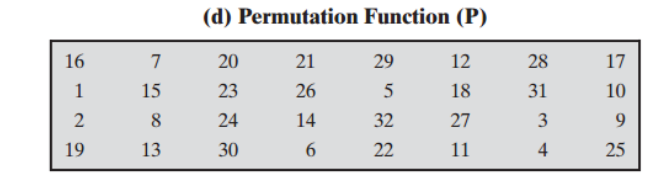
* **input:** 111001 111010 010011 000011 001111 110101 101000 101110
* **Chia nhỏ thành 8 cặp 6 bit**



|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **i** | **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** |
| **6 bit** | 111001 | 111010 | 010011 | 000011 | 001111 | 110101 | 101000 | 101110 |
| **S\_box** | 10 | 3 | 2 | 15 | 1 | 1 | 12 | 2 |
| **bin** | 1010 | 0011 | 0010 | 1111 | 0001 | 0001 | 1100 | 0010 |

* **Result S-box** = 1010 0011 0010 1111 0001 0001 1100 0010

**+ Permutation (P) (32bit):**

****

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **input** | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
| **key** | 1 | 0 | 1 | 0 | 0 | 0 | 1 | 1 | 0 |

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 |
| 0 | 1 | 0 | 1 | 1 | 1 | 1 | 0 | 0 | 0 |

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 |
| 1 | 0 | 0 | 0 | 1 | 1 | 1 | 0 | 0 | 0 |

|  |  |  |
| --- | --- | --- |
| 30 | 31 | 32 |
| 0 | 1 | 0 |

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **P** | 16 | 7 | 20 | 21 | 29 | 12 | 28 | 17 | 1 |
| **value** | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 1 |

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 15 | 23 | 26 | 5 | 18 | 31 | 10 | 2 | 8 | 24 |
| 1 | 0 | 1 | 0 | 0 | 1 | 0 | 0 | 1 | 1 |

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 14 | 32 | 27 | 3 | 9 | 19 | 13 | 30 | 6 | 22 |
| 1 | 0 | 0 | 1 | 0 | 0 | 1 | 0 | 0 | 0 |

|  |  |  |
| --- | --- | --- |
| 11 | 4 | 25 |
| 1 | 0 | 1 |

* **Result after P** = 1110 0000 1101 0010 0111 0010 0100 0101

**+ L-left** XOR **result P:**

**L-left =** 0101 1010 0000 0000 0101 1010 0000 0000

**Result P =** 1110 0000 1101 0010 0111 0010 0100 0101

* **Result = L-right new =** 1011 1010 1101 0010 0010 1000 0100 0101

**Vậy:**

* L-Left new = L-right = 0011 1100 1110 0000 0011 1100 0000 1111
* L-Right new = 1011 1010 1101 0010 0010 1000 0100 0101