# Proceso para la Generación de Subllaves Ki

| Key | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|---|---|---|
| 0x | | | | | | | | |
| | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |
| 0x | | | | | | | | |
| | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 |
| 0x | | | | | | | | |
| | 25 | 26 | 27 | 28 | 29 | 30 | 31 | 32 |
| 0x | | | | | | | | |
| | 33 | 34 | 35 | 36 | 37 | 38 | 39 | 40 |
| 0x | | | | | | | | |
| | 41 | 42 | 43 | 44 | 45 | 46 | 47 | 48 |
| 0x | | | | | | | | |
| | 49 | 50 | 51 | 52 | 53 | 54 | 55 | 56 |
| 0x | | | | | | | | |
| | 57 | 58 | 59 | 60 | 61 | 62 | 63 | 64 |
| 0x | | | | | | | | |

PC-1

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | 57 | 49 | 41 | 33 | 25 | 17 | 9 | 1 |
| | | | | | | | | |
| | 58 | 50 | 42 | 34 | 26 | 18 | 10 | 2 |
| C0 | | | | | | | | |
| | 59 | 51 | 43 | 35 | 27 | 19 | 11 | 3 |
| | | | | | | | | |
| | 60 | 52 | 44 | 36 | **63** | **55** | **47** | **39** |
| | | | | | | | | |
| | **31** | **23** | **15** | **7** | **62** | **54** | **46** | **38** |
| | | | | | | | | D0 |
| | **30** | **22** | **14** | **6** | **61** | **53** | **45** | **37** |
| | | | | | | | | |
| | **29** | **21** | **13** | **5** | **28** | **20** | **12** | **4** |
| | | | | | | | | |

**PC-2 para K1**

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 14 | 17 | 11 | 24 | 1 | 5 | 3 | 28 |
| | | | | | | | |
| 15 | 6 | 21 | 10 | 23 | 19 | 12 | 4 |
| | | | | | | | |
| 26 | 8 | 16 | 7 | 27 | 20 | 13 | 2 |
| | | | | | | | |
| 41 | 52 | 31 | 37 | 47 | 55 | 30 | 40 |
| | | | | | | | |
| 51 | 45 | 33 | 48 | 44 | 49 | 39 | 56 |
| | | | | | | | |
| 34 | 53 | 46 | 42 | 50 | 36 | 29 | 32 |
| | | | | | | | |

| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| C0= | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | 29 | 30 | 31 | 32 | 33 | 34 | 35 | 36 | 37 | 38 | 39 | 40 | 41 | 42 | 43 | 44 | 45 | 46 | 47 | 48 | 49 | 50 | 51 | 52 | 53 | 54 | 55 | 56 |
| D0= | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| C1= | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | 29 | 30 | 31 | 32 | 33 | 34 | 35 | 36 | 37 | 38 | 39 | 40 | 41 | 42 | 43 | 44 | 45 | 46 | 47 | 48 | 49 | 50 | 51 | 52 | 53 | 54 | 55 | 56 |
| D1= | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| C_= | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | 29 | 30 | 31 | 32 | 33 | 34 | 35 | 36 | 37 | 38 | 39 | 40 | 41 | 42 | 43 | 44 | 45 | 46 | 47 | 48 | 49 | 50 | 51 | 52 | 53 | 54 | 55 | 56 |
| D_= | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

**PC-2 para K_**

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 14 | 17 | 11 | 24 | 1 | 5 | 3 | 28 |
| | | | | | | | |
| 15 | 6 | 21 | 10 | 23 | 19 | 12 | 4 |
| | | | | | | | |
| 26 | 8 | 16 | 7 | 27 | 20 | 13 | 2 |
| | | | | | | | |
| 41 | 52 | 31 | 37 | 47 | 55 | 30 | 40 |
| | | | | | | | |
| 51 | 45 | 33 | 48 | 44 | 49 | 39 | 56 |
| | | | | | | | |
| 34 | 53 | 46 | 42 | 50 | 36 | 29 | 32 |
| | | | | | | | |

K1= 0x _ _ _ _ _ _ _ _ _ _ _ _

K_= 0x _ _ _ _ _ _ _ _ _ _ _ _