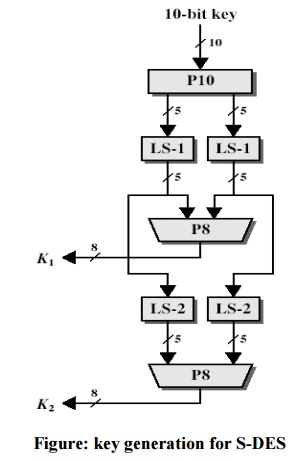


workflow for Encryption and Decryption



P10(Permutate)

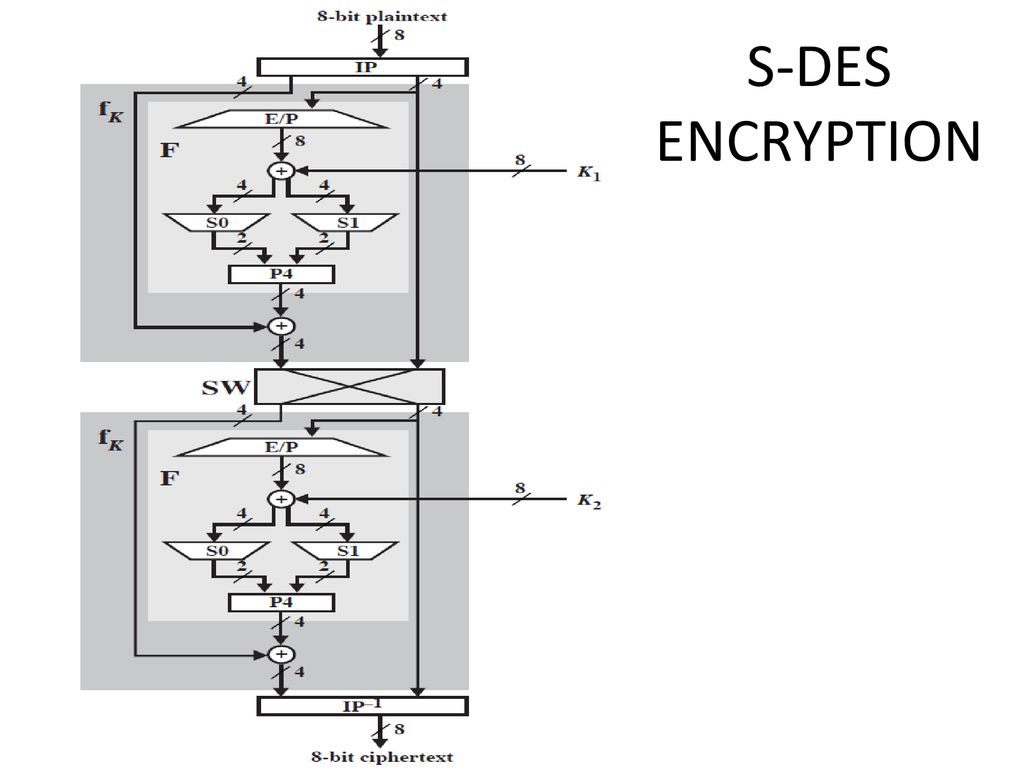
|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| 3 | 5 | 2 | 7 | 4 | 10 | 1 | 9 | 8 | 6 |

P8(Select and Permutate)

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| 6 | 3 | 7 | 4 | 8 | 5 | 10 | 9 | - | - |

P4(Permutate)

|  |  |  |  |
| --- | --- | --- | --- |
| 1 | 2 | 3 | 4 |
| 2 | 4 | 3 | 1 |



EP(Expand and Permutate)

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | 2 | 3 | 4 |  |  |  |  |
| 4 | 1 | 2 | 3 | 2 | 3 | 4 | 1 |

IP(Initial Permutation)

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| 2 | 6 | 3 | 1 | 4 | 8 | 5 | 7 |

IP(Inverse)

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| 4 | 1 | 3 | 5 | 7 | 2 | 8 | 6 |

Substitution Box

