



PP = Počáteční permutace PP⁻¹ = Konečná permutace

Obr. 5.1 Algoritmus DES