



**Figure 3.4** General  $n$ -bit- $n$ -bit Block Substitution (shown with  $n = 4$ )