Abstract: We discuss different types of distinguishing attacks on symmetric key designs, namely pseudorandom function (or permutation) and others. We study the classical methods (e.g., Davies-Meyer, Even-Mansoor etc.) of pseudorandom functions and permutations based on a block cipher or an ideal permutation. We explore some recent cryptanalysis development on composition-type designs.