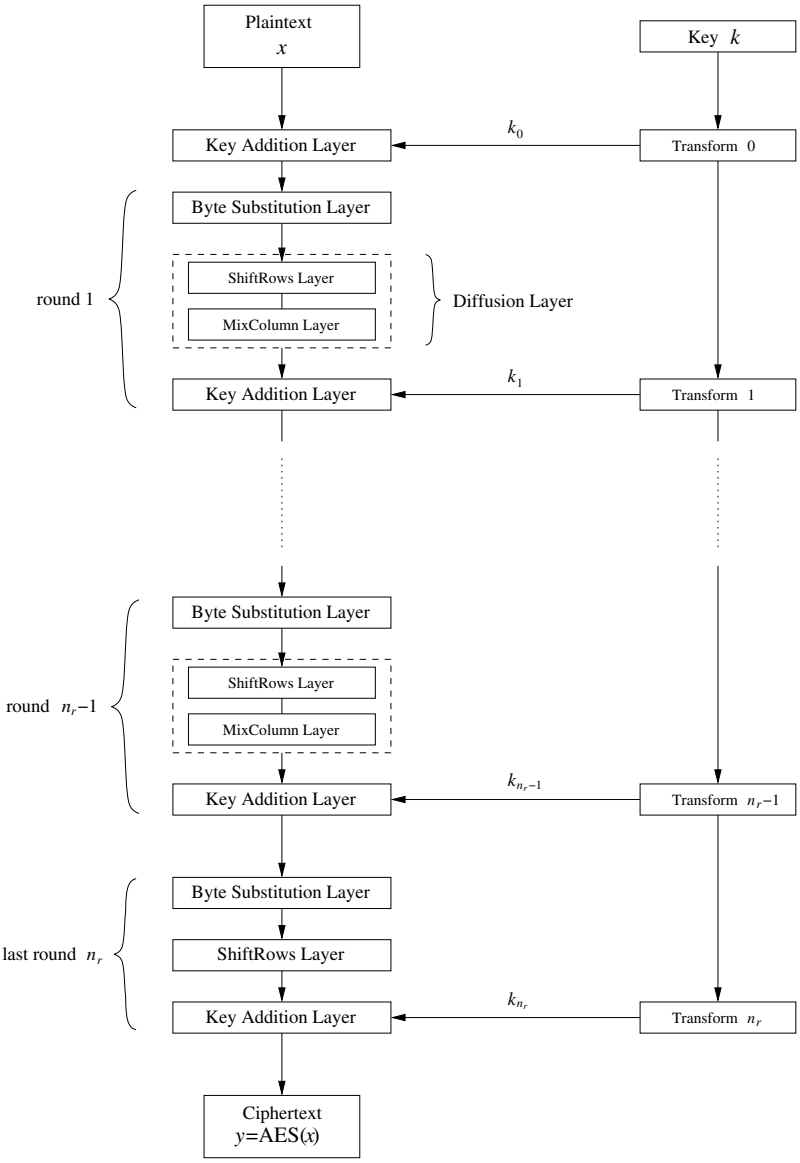

Fig. 4.2 AES encryption block diagram

can add, subtract, multiply and invert. Before we introduce the definition of a field, we first need the concept of a a simpler algebraic structure, a group.