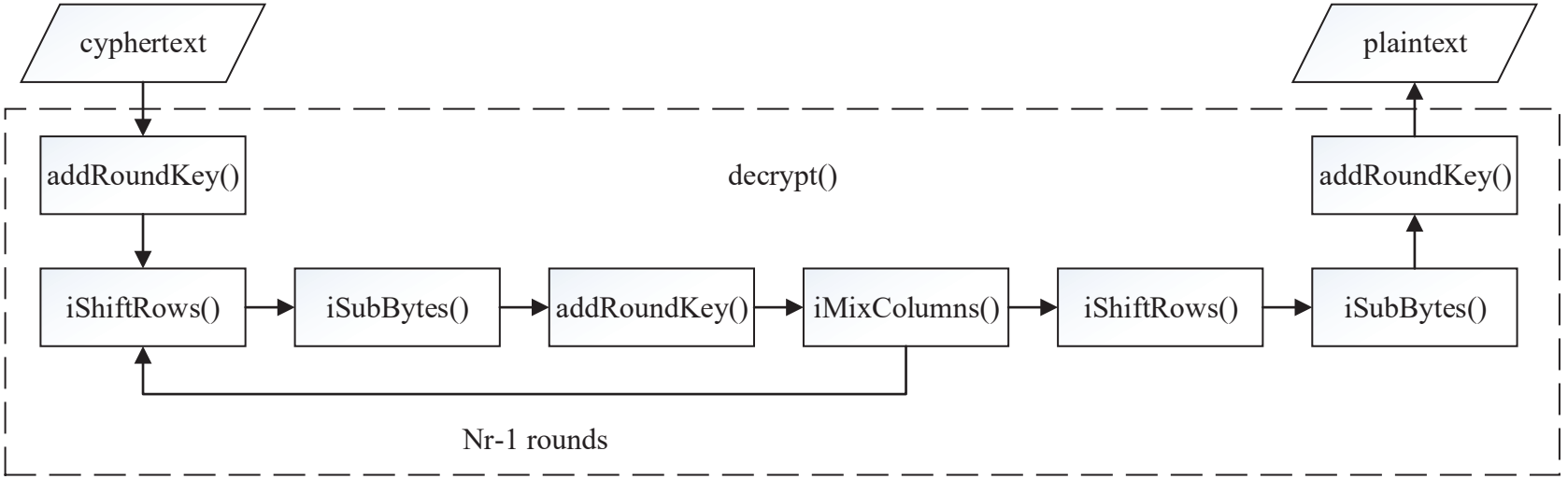
cyphertext
plaintext
addRoundKey()
decrypt()
addRoundKey()
iShiftRows()
iSubBytes()
addRoundKey()
iMixColumns()
iShiftRows()
iSubBytes()
Nr-1 rounds