线性攻击小结：

线性密码分析是对称加密算法的一种有效攻击方式，它利用加密算法中的线性关系，通过构建线性逼近表达式来推测密钥。攻击者需收集大量明密文对，计算这些线性表达式的实际概率，并与随机猜测的概率进行比较，以评估其有效性。

然而，对DES算法实施线性攻击面临一些挑战：一是获取足够多的明密文对非常困难，二是DES算法的密钥空间巨大（2^56种可能），需要极大量的独立线性表达式和统计分析才能逐步缩小密钥搜索范围，这导致计算密集且耗时极长。尽管线性密码分析在理论上为破解DES提供了路径，但在实践中，其成功实施受限于数据获取难度、计算资源限制和时间成本。现代加密算法如AES在设计时已增强了抵抗此类攻击的能力。

在代码实现模拟攻击中，我通过随机生成明文和密钥来获取一些明密文对，并且缩小密钥空间来模拟攻击。但是没有大量的明密文对，且缩小了密钥空间，导致找到的最佳密钥候选得分较低，无法找到正确的密钥。虽然无法实现真正的对DES算法进行线性攻击，但是这个实验使我了解了对DES算法实施线性攻击的原理与实现的可能性。

（各代码作用）

（一）des\_create.py生成明密文对

·主要用于为DES的线性攻击提供明密文对以便进行分析

（二）DES\_s\_linear.py 针对数据加密标准（DES）算法中的S盒进行线性分析

·主要用于构建和分析 S 盒的线性逼近表，这是线性密码分析的核心步骤之一。

（三）des\_L.py

·根据DES\_s\_linear.py所得到的结果构建线性近似表，是攻击的第一步，提供了关于 DES S 盒行为的详细信息。

·遍历可能的密钥并对每个密钥进行评分，是攻击的关键，它量化了每个密钥候选与已知明文-密文对之间的匹配程度。

·寻找最佳密钥候选，是最终目标，即找到最有可能揭示真实密钥一部分的候选。