|  |  |  |
| --- | --- | --- |
| **关卡内容** | **过关情况文字描述** | **图片演示** |
| **第1关：基本测试**  根据S-DES算法编写和调试程序，提供GUI解密支持用户交互。输入可以是8bit的数据和10bit的密钥，输出是8bit的密文。 | 实现了完整的 S-DES 算法核心逻辑（SDES类），包含置换、移位、子密钥生成、Feistel 轮函数等关键步骤，支持 8 位二进制数据与 10 位密钥的加解密。  通过SDESGUI类的 “基本加密解密” 标签页提供 GUI 交互，用户可输入明文 / 密文和密钥，点击按钮直接获取加密 / 解密结果，输出为 8 位二进制密文 / 明文，满足交互需求。 | 9eee9b5c1f8ad7ba67c4cd09c44a71ee |
| **第2关：交叉测试**  考虑到是**算法标准**，所有人在编写程序的时候需要使用相同算法流程和转换单元(P-Box、S-Box等)，以保证算法和程序在异构的系统或平台上都可以正常运行。  设有A和B两组位同学(选择相同的密钥K)；则A、B组同学编写的程序对明文P进行加密得到相同的密文C；或者B组同学接收到A组程序加密的密文C，使用B组程序进行解密可得到与A相同的P。 | 严格遵循 S-DES 算法标准，代码中定义了固定的置换盒（P10、P8、IP 等）、S 盒（S1\_BOX、S2\_BOX）及移位规则，确保所有开发者使用相同的转换单元。  算法流程完全一致（如子密钥生成步骤、两轮 Feistel 网络的顺序与逻辑），因此不同平台的程序使用相同密钥时，对同一明文加密结果相同，解密也能还原原始明文，满足异构系统兼容性。 |  |
| **第3关：扩展功能**  考虑到向实用性扩展，加密算法的数据输入可以是ASII编码字符串(分组为1 Byte)，对应地输出也可以是ACII字符串(很可能是乱码)。 | 通过SDES类的str\_to\_bin\_list和bin\_list\_to\_str方法，实现 ASCII 字符串与 8 位二进制块的转换。  提供encrypt\_str和decrypt\_str方法，支持对 ASCII 字符串按字节分组加密 / 解密，输出为 ASCII 字符串（可能是乱码），并在 “字符串加密解密” 标签页提供对应交互，实现实用性扩展。 | 6c969d2140de5e91ef580ee0378fd623 |
| **第4关：暴力破解**  假设你找到了使用相同密钥的明、密文对(一个或多个)，请尝试使用暴力破解的方法找到正确的密钥Key。在编写程序时，你也可以考虑使用多线程的方式提升破解的效率。请设定时间戳，用视频或动图展示你在多长时间内完成了暴力破解。 | SDES.brute\_force方法遍历所有可能的 10 位密钥（共 1024 种），对给定明密文对进行匹配测试，返回所有有效密钥。  采用多线程机制（threading.Thread）执行破解任务，避免阻塞 GUI 界面，并通过进度条实时展示破解进度。  记录破解耗时（time.time()计算），可通过结果中的时间戳验证破解效率，满足时间展示要求。 | 15e9a7f4a8d4193e2a171dbf55ac5dd6 |
| **第5关：封闭测试**  根据第4关的结果，进一步分析，对于你随机选择的一个明密文对，是不是有不止一个密钥Key？进一步扩展，对应明文空间任意给定的明文分组[P\_{n}](" \l ")，是否会出现选择不同的密钥[K\_{i}\ne K\_{j}](" \l ")加密得到相同密文[C\_n](" \l ")的情况？ | 暴力破解结果会显示所有匹配的密钥，若存在多个密钥（count > 1），则明确提示 “S-DES 存在密钥碰撞现象”。  代码逻辑隐含对加密碰撞的验证：通过遍历所有密钥，可发现不同密钥（K\_i ≠ K\_j）对同一明文加密可能得到相同密文，直接支持对 “密钥碰撞是否存在” 的分析结论。 |  |