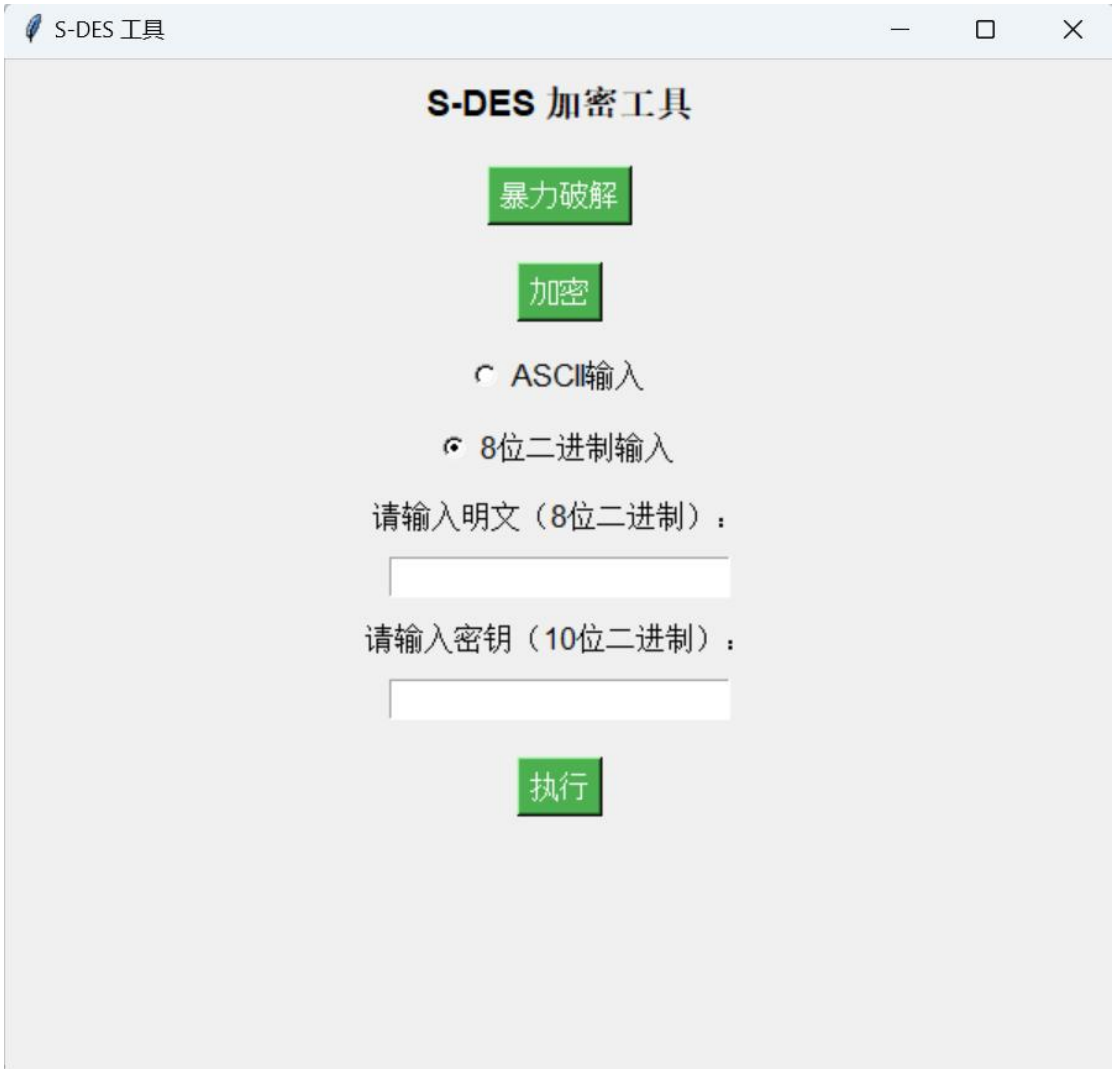
测试结果

1.第一关：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。

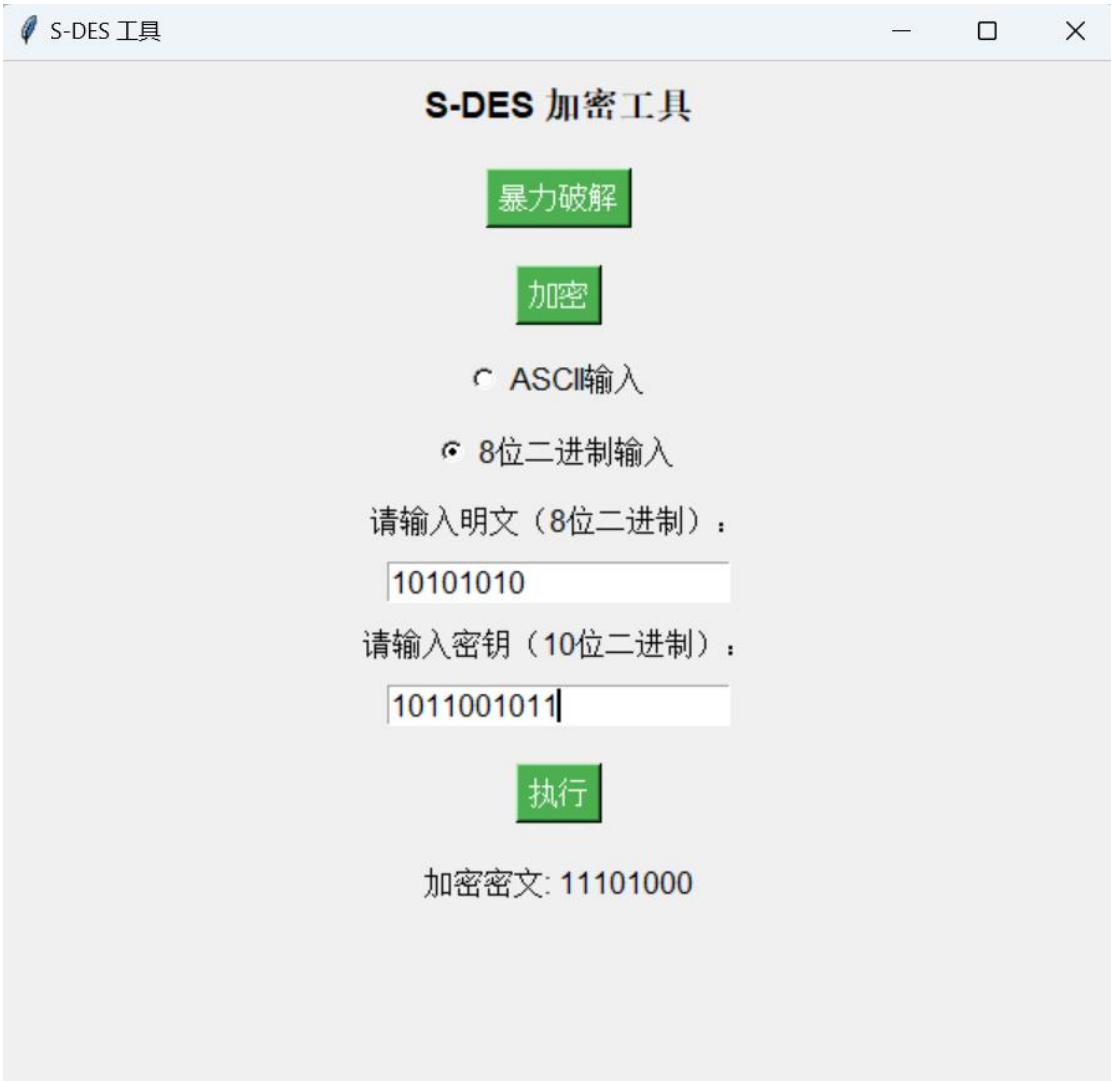
1.1 用户交互界面

在“请输入明文（8 位二进制）”和“请输入密钥（10 位二进制）：”下方的输入框分别手动输入明文和密钥，点击下方“执行”按钮生成 8 位密文



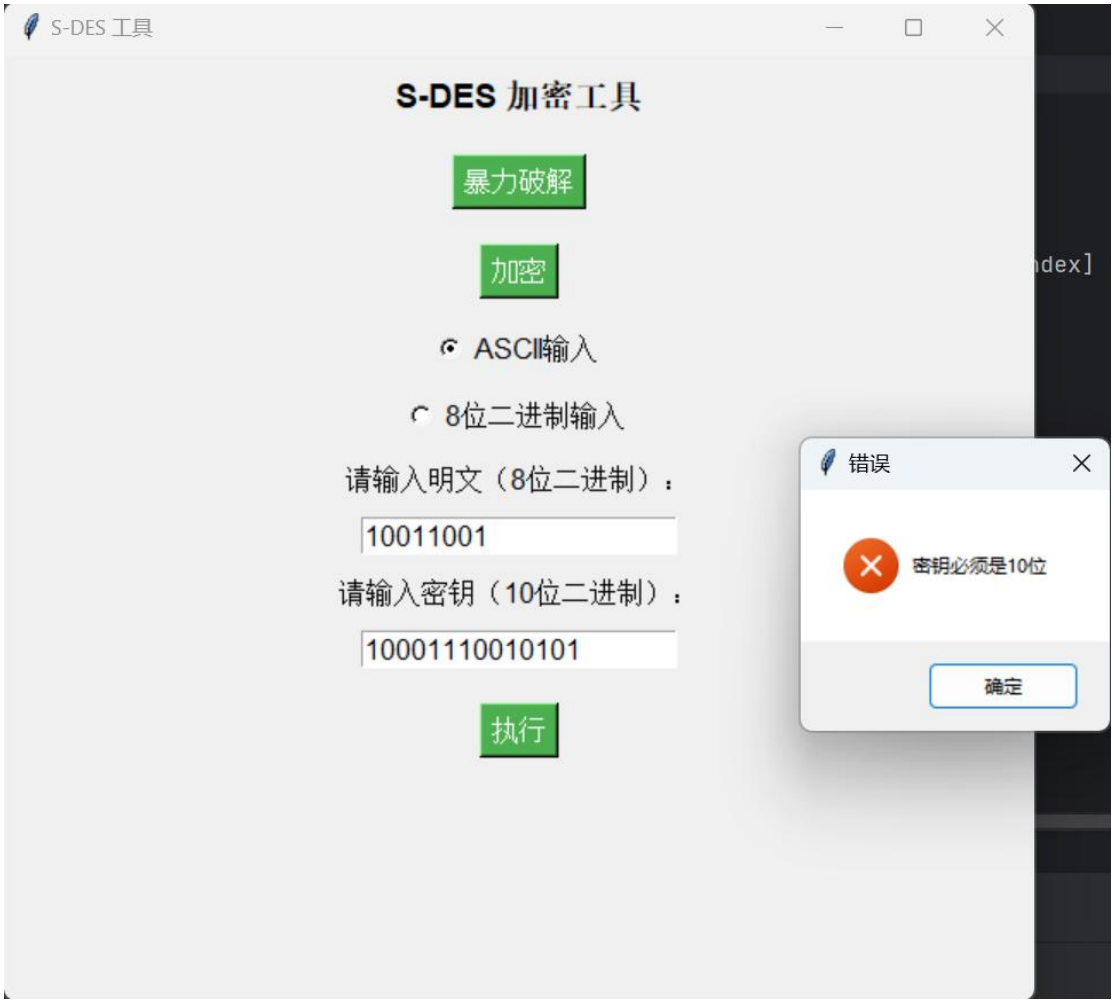
1.2 加密测试结果

明文：10101010
密钥：1011001011
求得密文：11101000



1.3 异常处理测试

输入的明文或密钥不符合规范时，将弹出异常提醒窗口，加密无法执行



1.4 总结

在本关卡中，我们小组成功完成了任务，主要体现在以下几个方面：
①S-DES 算法的理解与实现：我们深入理解了 S-DES 算法的基本概念，包括初始置换、轮函数、S 盒和 P 盒，并编写了程序，能够根据 8 位数据和 10 位密钥执行 S-DES 的加密和解密。
②GUI 设计与用户交互：我们创建了一个用户友好的图形界面，设计了文本输入框和按钮，使用户可以输入数据和密钥，并选择进行加密或解密，从而提升了程序的可用性和用户体验。
③加密与解密功能的实现：实现了 S-DES 算法的加解密功能，并进行了系统测试和调试，以确保程序能够准确处理不同情况，从而保证其正确性和稳定性。
④用户友好性和错误处理：我们重视界面的易用性，并提供了错误提示和反馈机制，以帮助用户解决问题，从而提升了程序的友好性。

2.第二关：交叉测试

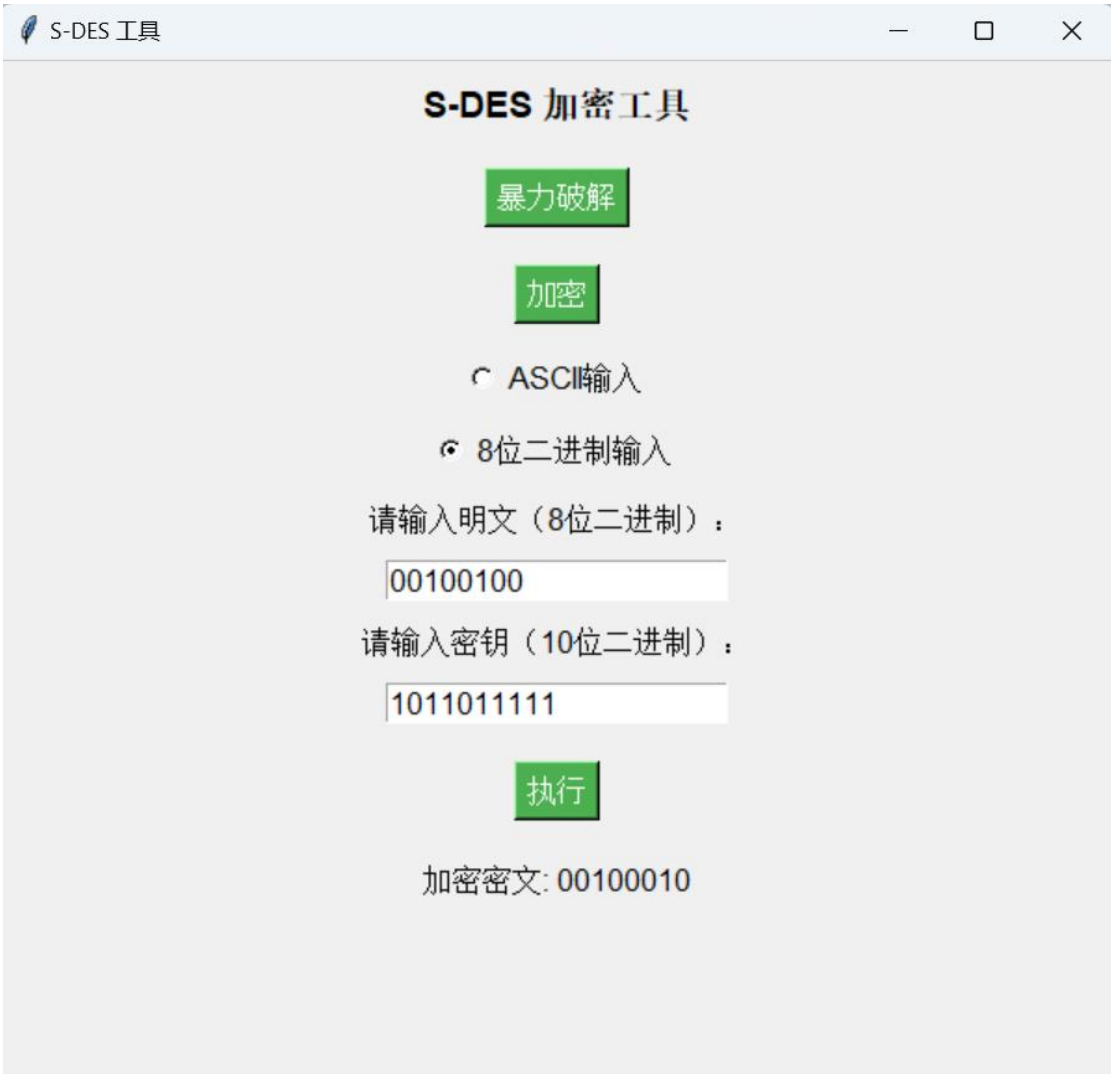
考虑到是**算法标准**，所有人在编写程序的时候需要使用相同算法流程和转换单元(P-Box、S-Box 等)，以保证算法和程序在异构的系统或平台上都可以正常运行。

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。

2.1 我方主动加密，由对方进行协作测试

2.1.1 我方加密结果

密钥：1011011111
原文：10101010
密文：00100100

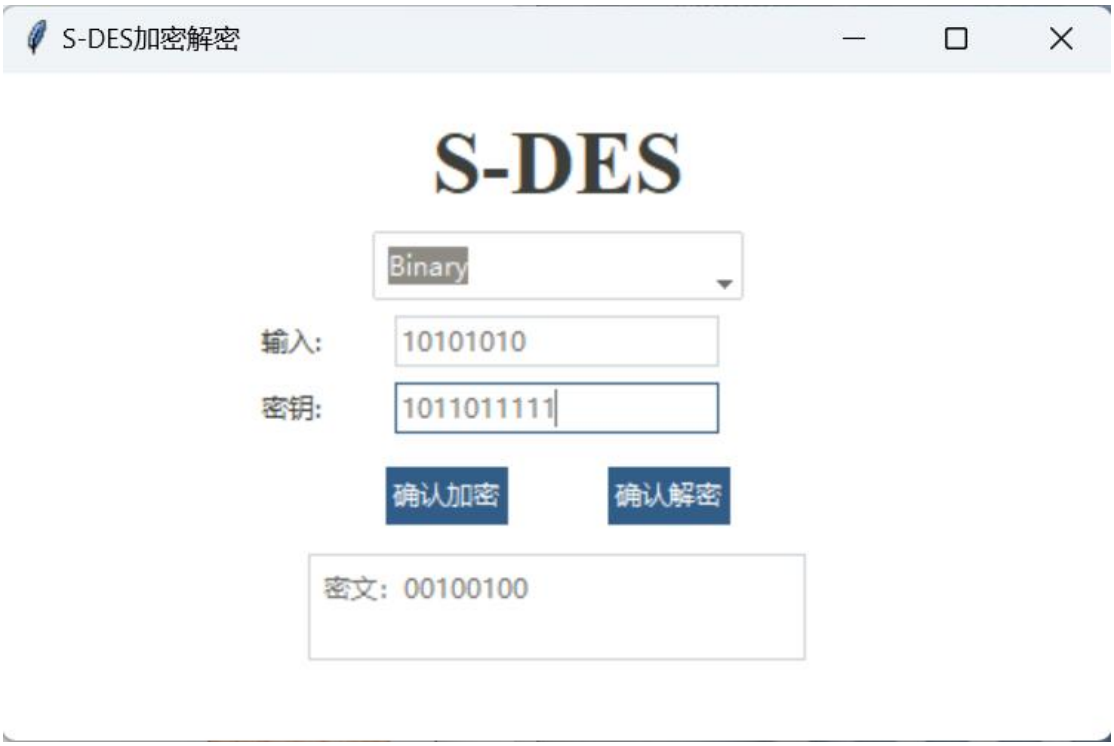


2.1.2 对方加密结果

密钥：1011011111

原文：10101010

密文：00100100

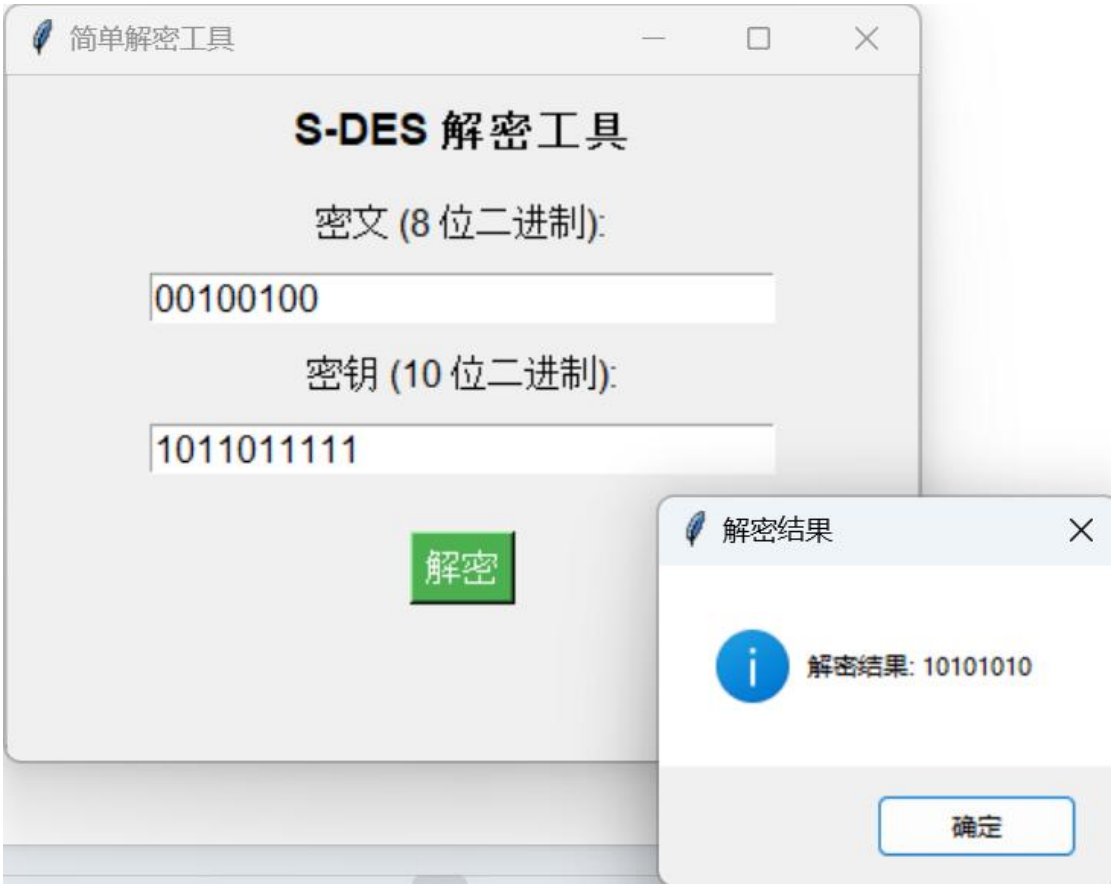


2.1.3 我方解密结果

密钥：1011011111

密文：00100100

原文：10101010

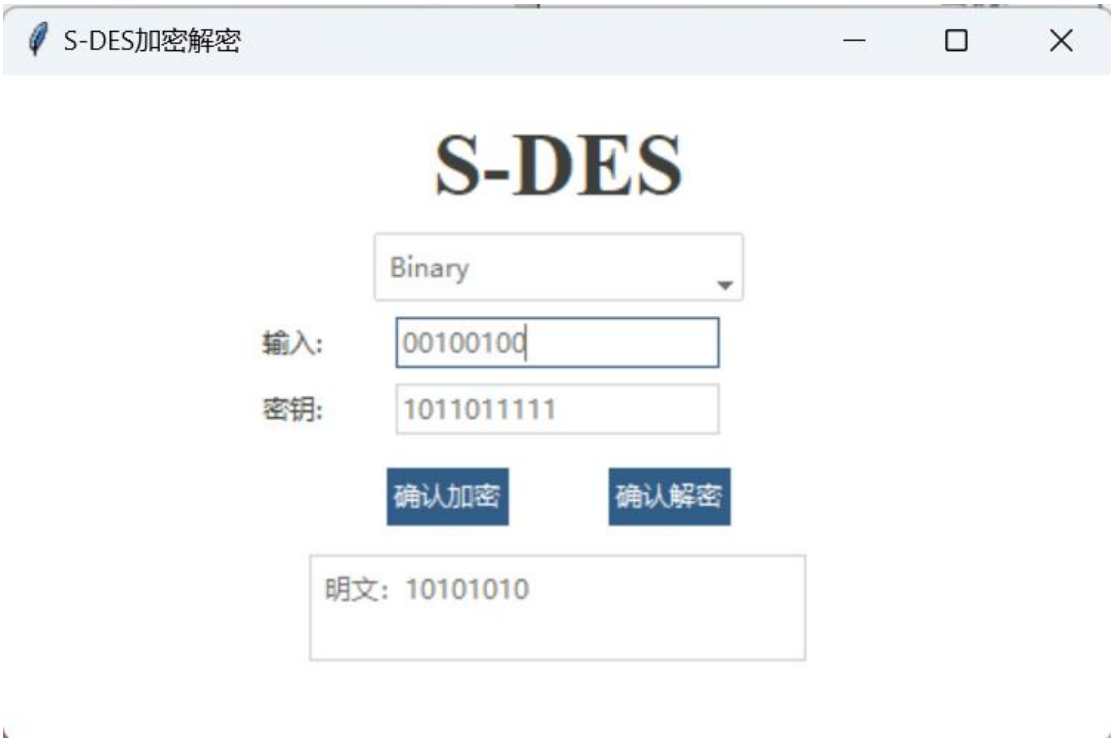


2.1.4 对方解密结果

密钥：1011011111

密文：00100100

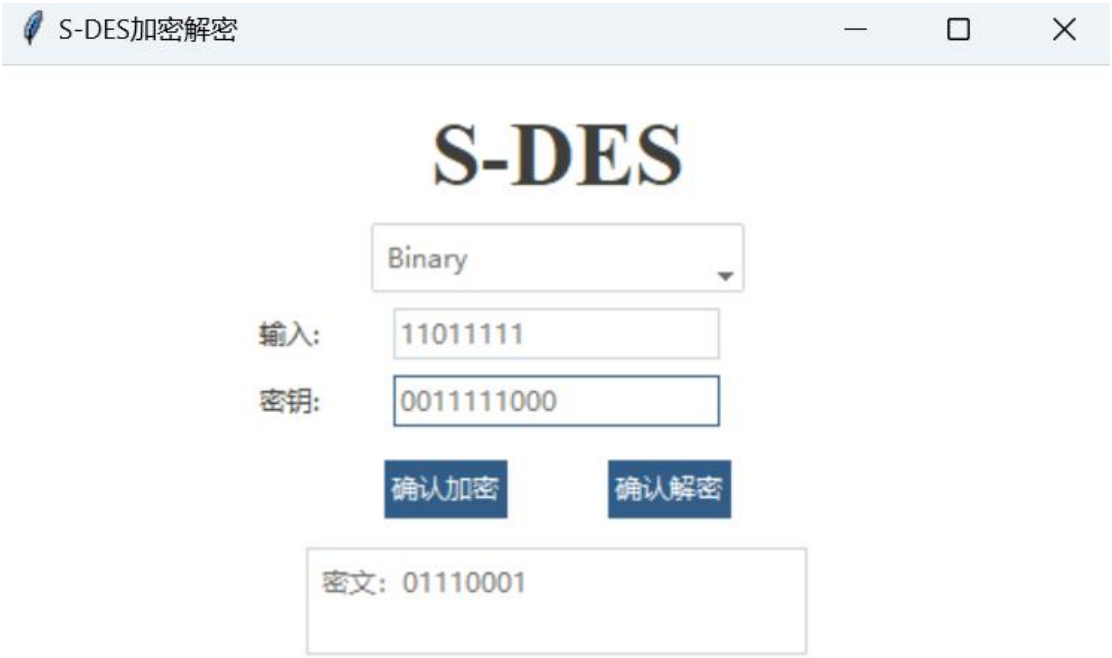
原文：10101010



2.2 对面主动加密，由我方进行协作测试

2.2.1 对方加密结果

密钥：0001111000
原文：11011111
密文：01011101

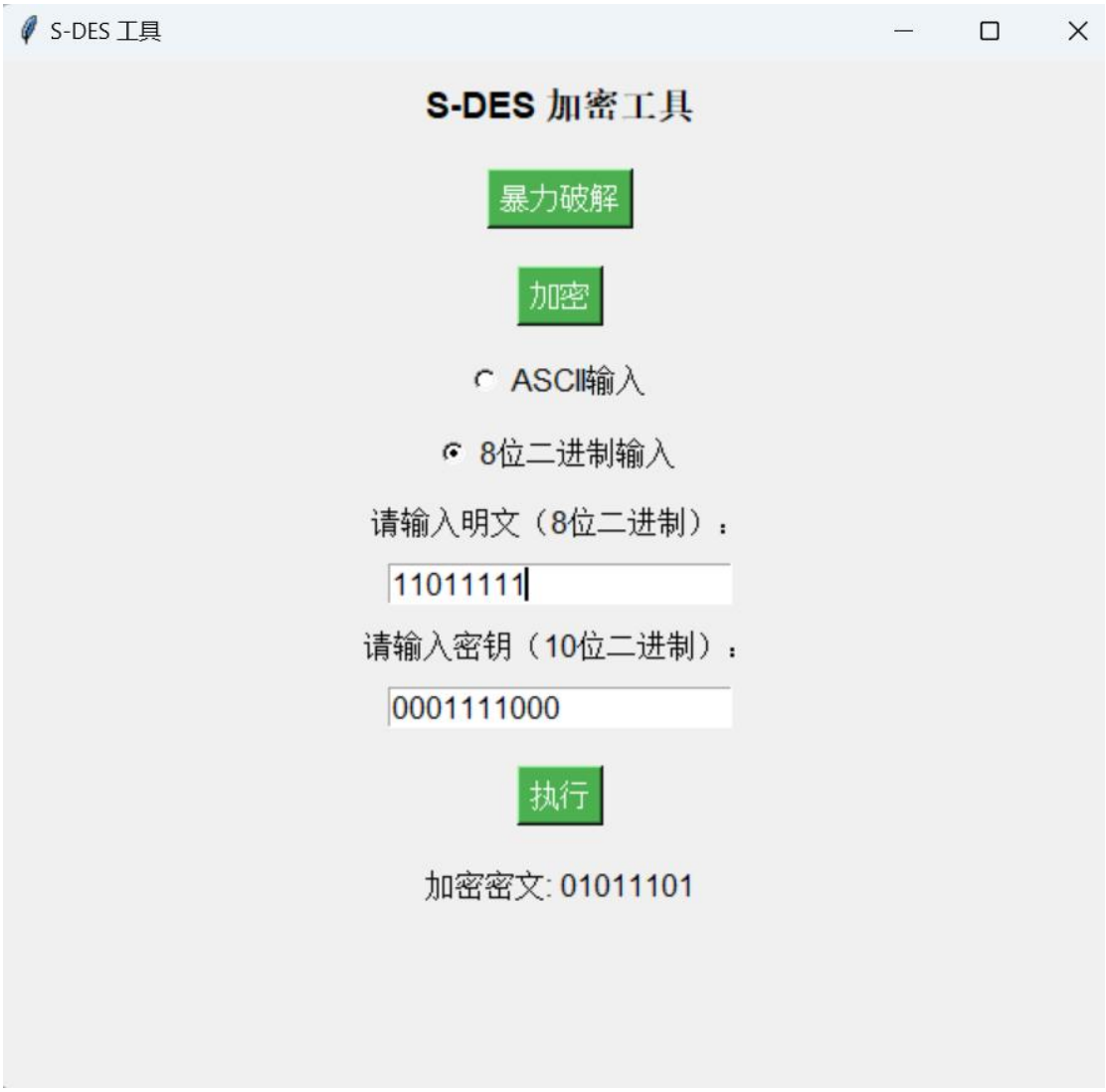


2.2.2 我方加密结果

密钥：0001111000

原文：11011111

密文：01011101

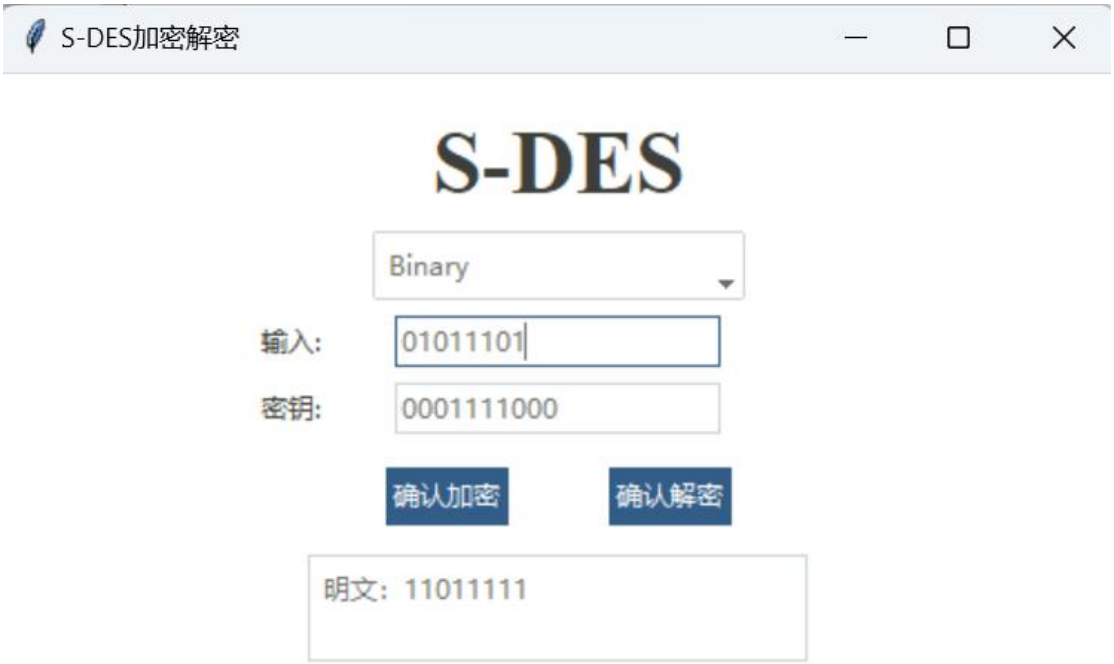


2.2.3 对方解密结果

密钥：0001111000

密文：01011101

原文：11011111

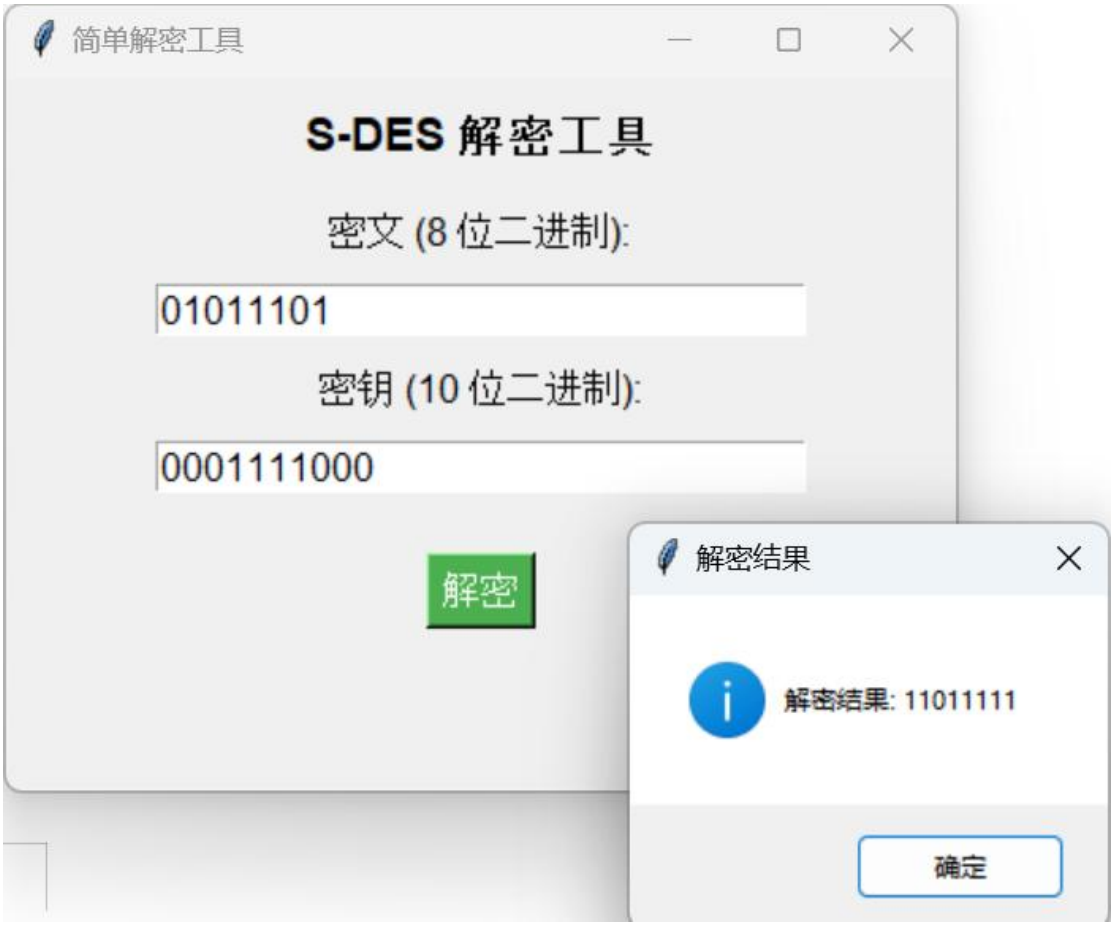


2.2.4 我方解密结果

密钥：0001111000

密文：01011101

原文：11011111



2.3 总结

在本关卡中，我们其他小组成功进行了交叉测试，结果表明在相同密钥下，加密和解密的结果一致且准确。我们主要达成了以下几个目标：
①理解算法标准化的重要性：通过此次实验，我们深刻认识到算法标准化的意义，确保不同开发者能够使用统一的算法流程和转换单元进行数据加解密，是保障信息安全和数据一致性的关键。
②遵循一致的算法规范：实验中，我们两组遵循了相同的算法规范，包括使用相同的密钥 K、P-Box 和 S-Box。这确保了生成的密文 C 是一致的。
③成功生成一致的密文：本实验的核心目标是确保 A 组与 B 组编写的程序能够生成相同的密文 C。通过一致的密钥 K 和算法，我们成功实现了这一点，确保无论是 A 组加密由 B 组解密，还是反向操作，都能得到相同的原始明文 P。
④强调算法的异构性与跨平台性：实验突出了算法在不同平台间的兼容性，这在信息安全领域尤为重要，因为它确保各系统和平台上的程序能够正确处理数据，避免不一致或错误的结果。
⑤加深对信息安全的理解：此次实验让我更深入了解信息安全的一些基本概念，包括加密算法的实际应用、密钥管理以及算法标准化的重要性，这将帮助我更好地应对未来的信息安全挑战。

3.第 3 关：扩展功能

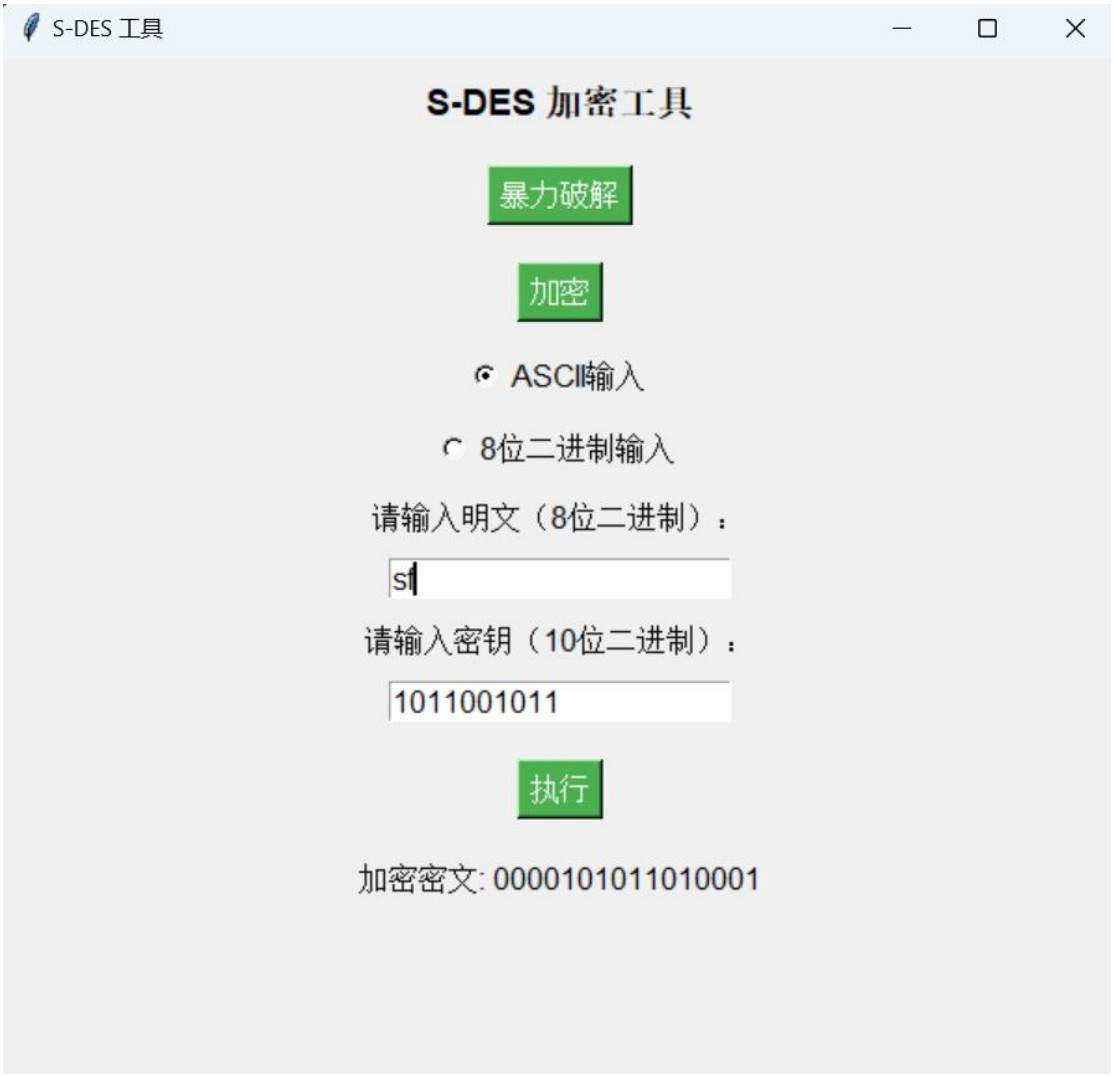
考虑到向实用性扩展，加密算法的数据输入可以是 ASII 编码字符串(分组为 1 Byte)，对应地输出也可以是 ACII 字符串(很可能是乱码)。

3.1 加密测试

密钥：1000101110

明文：sf

求得密文：0000101011010001



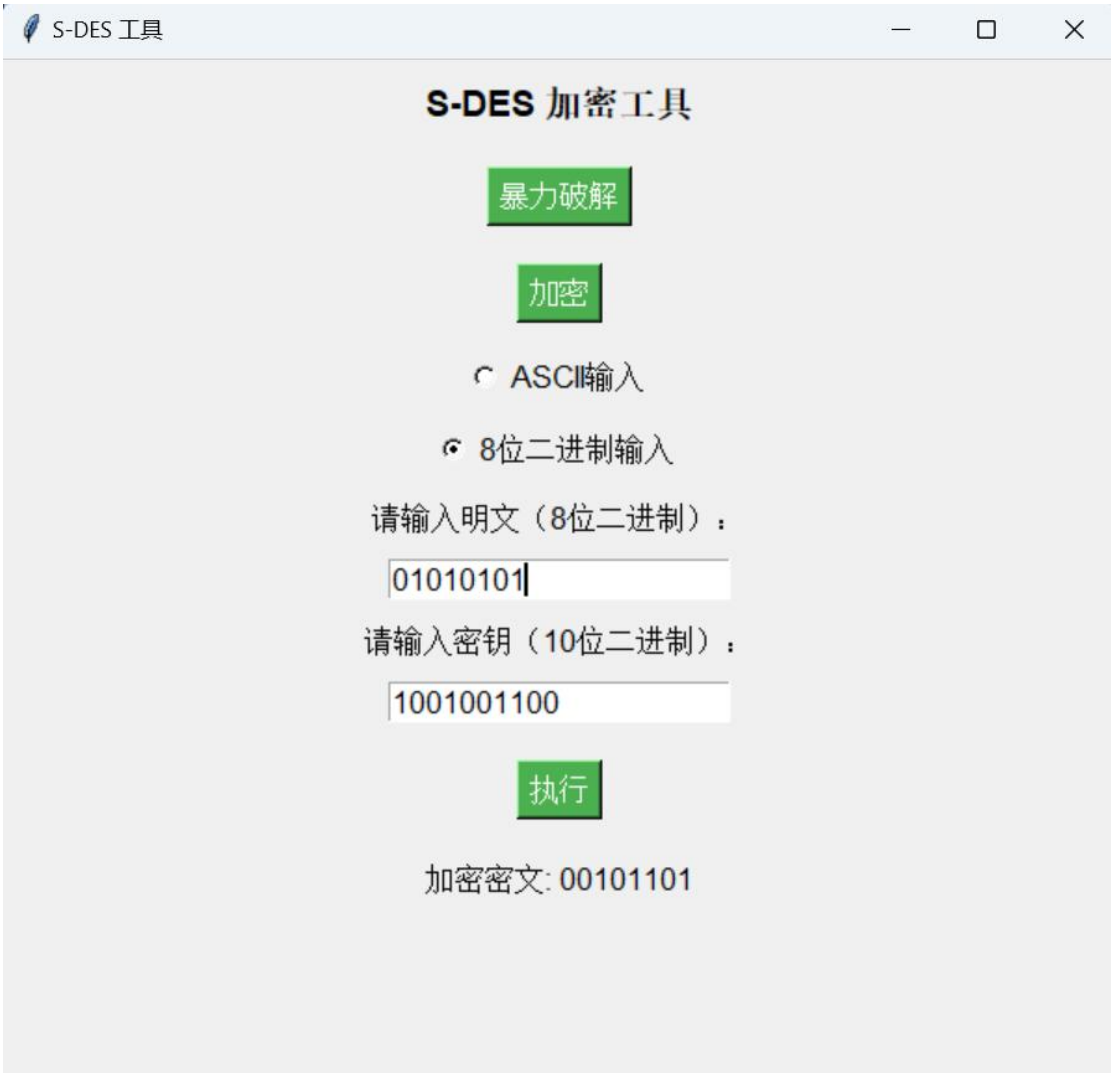
3.2 总结

在实验中，我们成功地修改了加密算法，以接受 ASCII 编码的字符串输入，每个字符表示一个字节。这允许用户输入文本数据，而不是传统的二进制数据。

4. 第 4 关：暴力破解

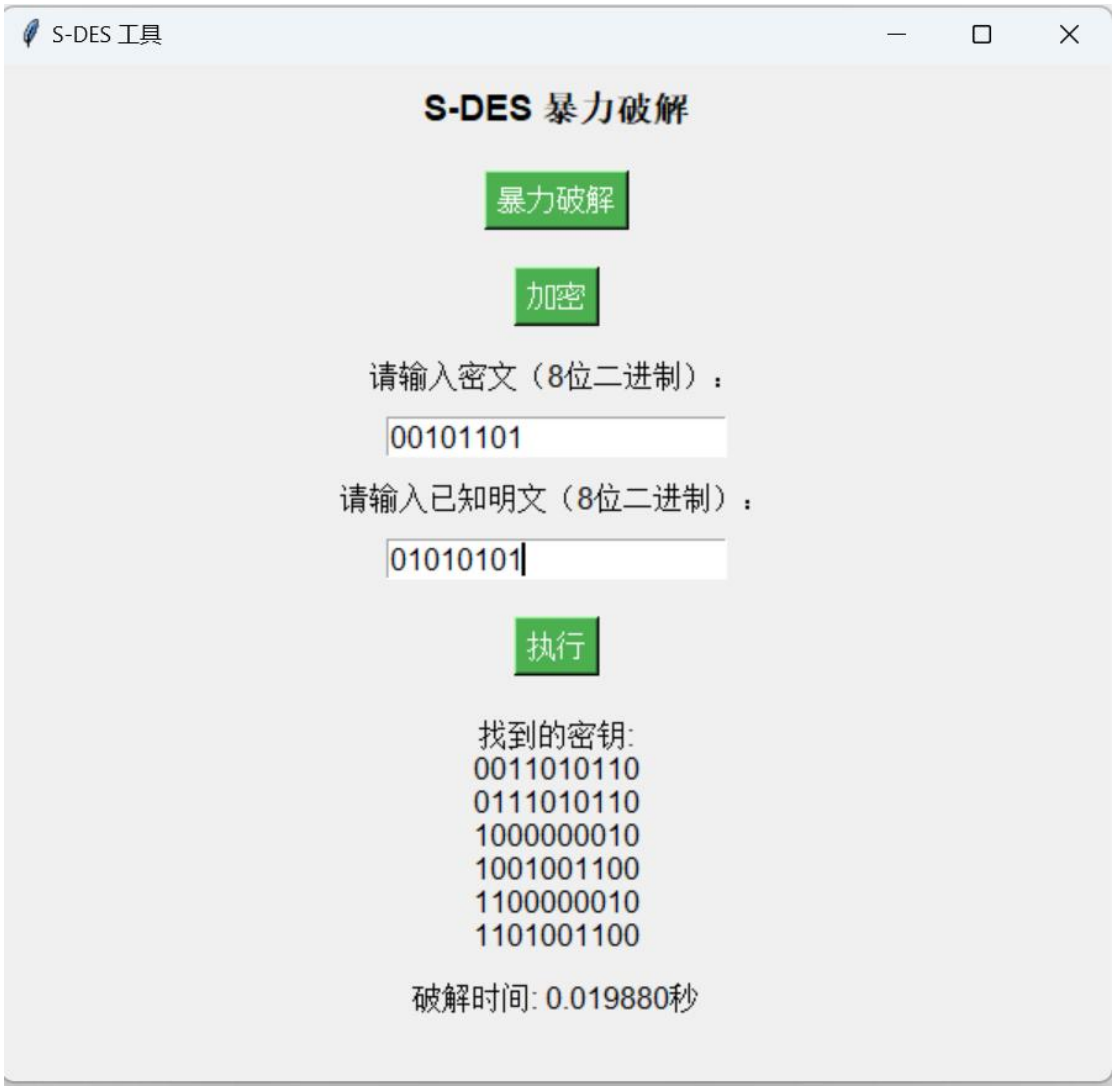
假设你找到了使用相同密钥的明、密文对(一个或多个)，请尝试使用暴力破解的方法找到正确的密钥 Key。在编写程序时，你也可以考虑使用多线程的方式提升破解的效率。请设定时间戳，用视频或动图展示你在多长时间内完成了暴力破解。

4.1 生成一组明文密文



4.2 破解测试

破解所得可能的密钥：
①0011010110
②0111010110
③1000000000
④1001001100
⑤1100000010
⑥1101001100



4.3 总结

在本关卡中，我们小组对随机生成的一组明文和密文进行了暴力破解，成功获得了可能的密钥。我们发现符合条件的密钥不止一组。在这一过程中，我们主要实现了以下目标：
①了解暴力破解：通过实验，我们深入认识了暴力破解攻击的原理。这种方法依

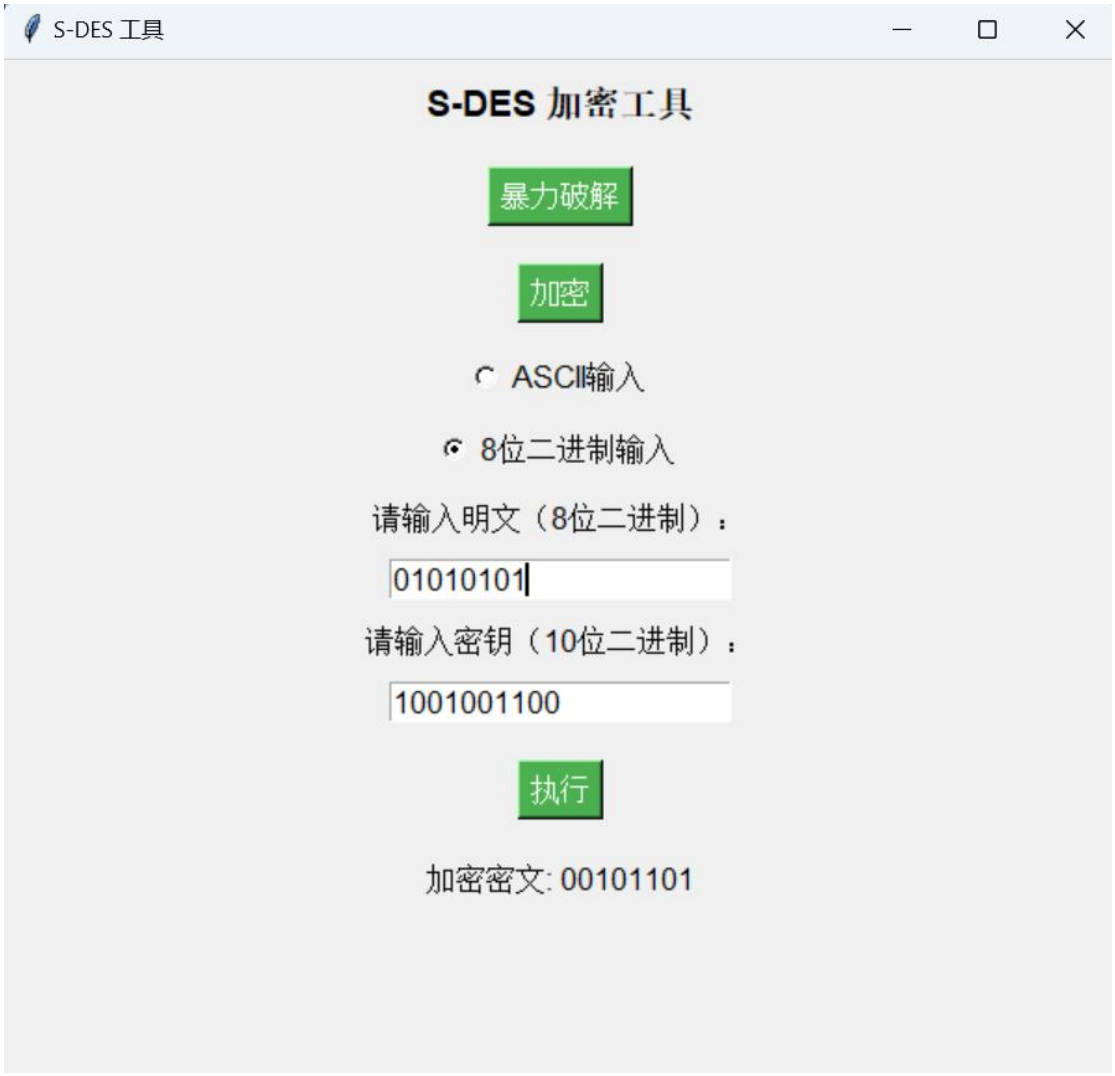
靠穷举所有可能的密钥组合来找到正确的密钥，从而增强了我对密码学的重要性、密钥强度和安全性概念的理解。
②多线程优化：我们成功地应用多线程技术来提升破解效率。这一实用技巧能够加快密钥搜索，尤其在处理大密钥空间时，具有重要意义，对于实际应用中的密码破解和安全性评估尤为关键。
③时间戳记录：为了展示破解所需的时间成本，我们记录了整个过程的时间戳。这有助于我们理解破解复杂密钥的耗时，以及评估不同安全级别密码系统的重要性。
④密码学原理的应用：此实验突出了密码学原理的实际应用。我们不仅学习了破解密钥的方法，还了解到如何保护密钥和数据以防范暴力破解攻击，这对未来在信息安全领域的工作非常有价值。

5.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，是否会出现选择不同的密钥 $K_i \neq K_j$ 加密得到相同密文 C_n 的情况？

5.1 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？

选取明密文对：01010101（明文）与 00101101（原文）



经过暴力破解得到的可能的密钥为：

①0011010110；

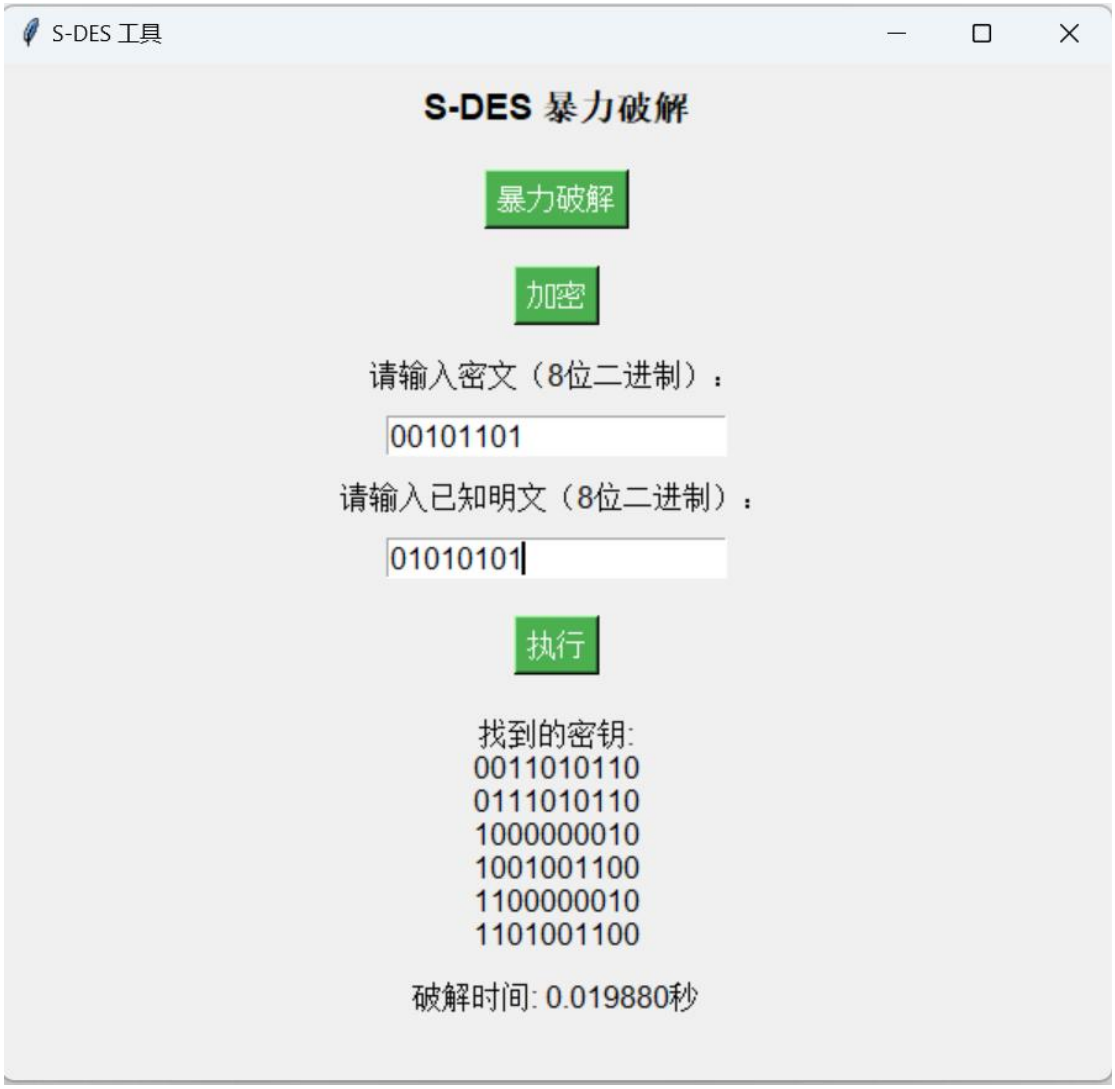
②0111010110；

③1000000000；

④1001001100；

⑤1100000010；

⑥1101001100。



由此可知，对于每一对明文和密文，只有一个特定的密钥（Key）可以生成对应的密文 C。加密算法的主要目标是确保密文 C 与相应的密钥 Key 相联系，从而保护数据的安全。因此，现代加密算法设计密钥时，通常会确保其唯一性，以实现加密和解密的独特性和可逆性。

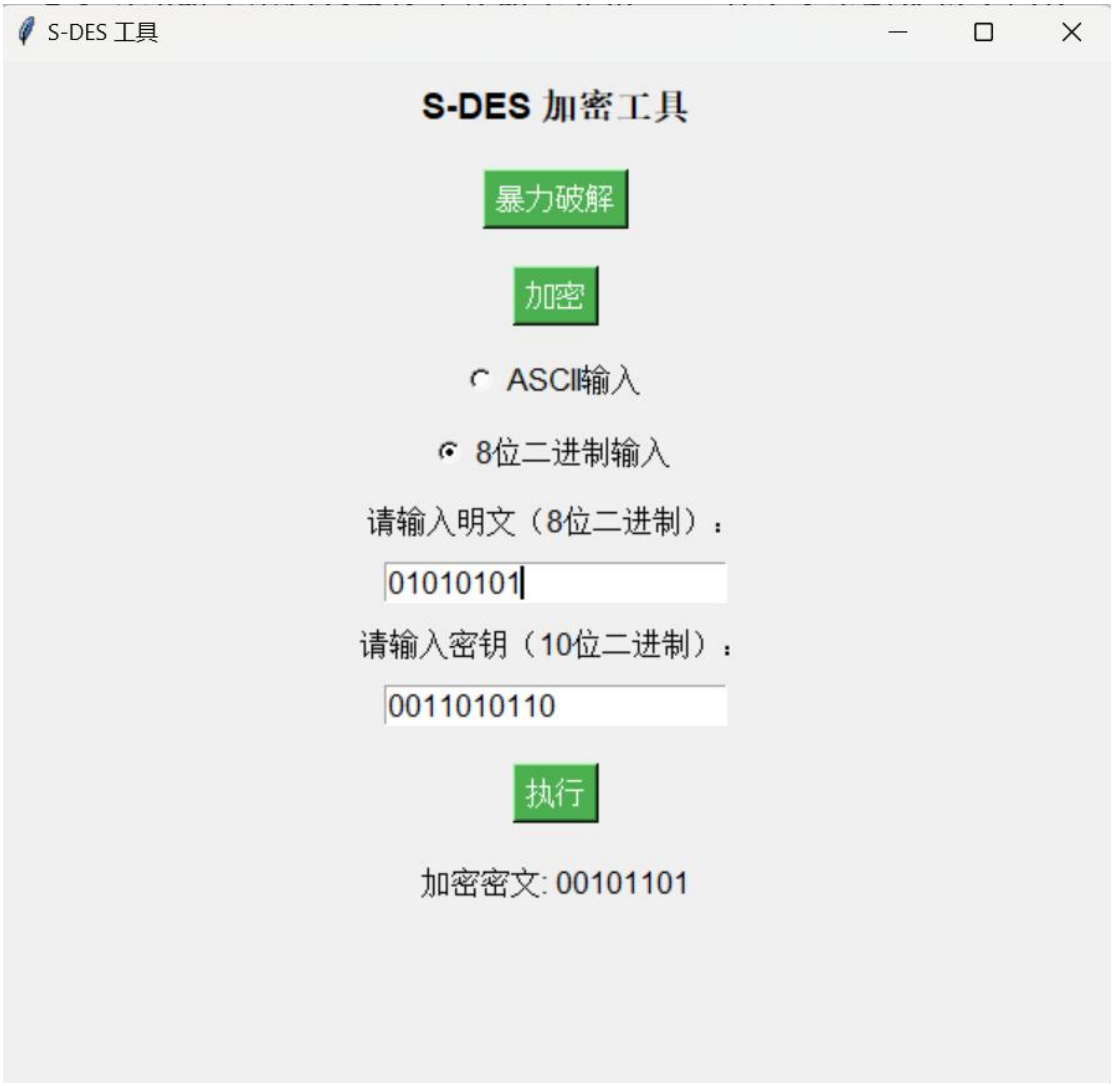
5.2 对应明文空间任意给定的明文分组 Pn，是否会出现选择不同的密钥 Ki≠Kj 加密得到相同密文 Cn 的情况？

利用以上获得的密钥进行测试，得到如下结果：

① 密钥：0011010110

原文：01010101

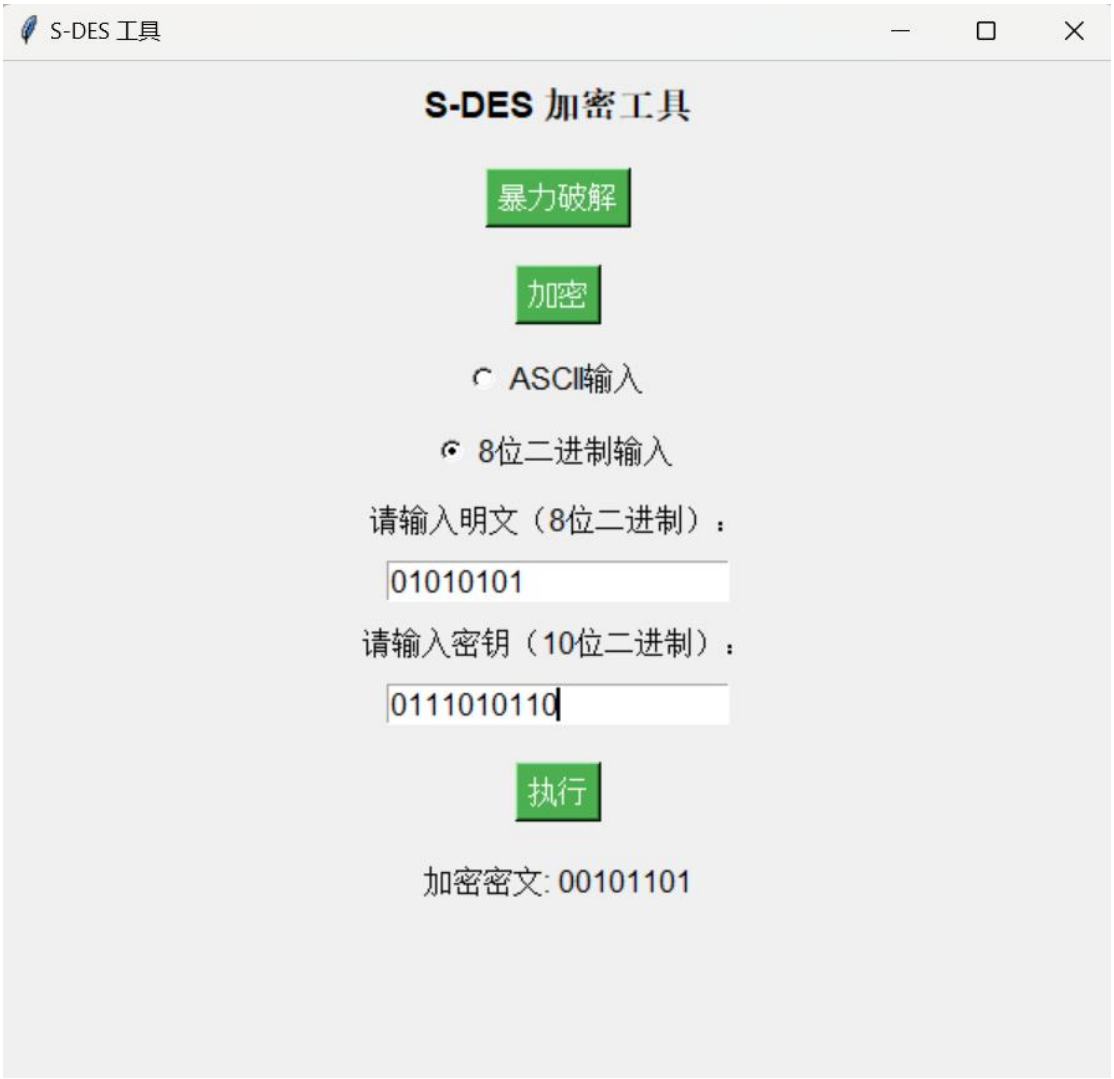
所得密文：00101101



② 密钥：0111010110

原文：01010101

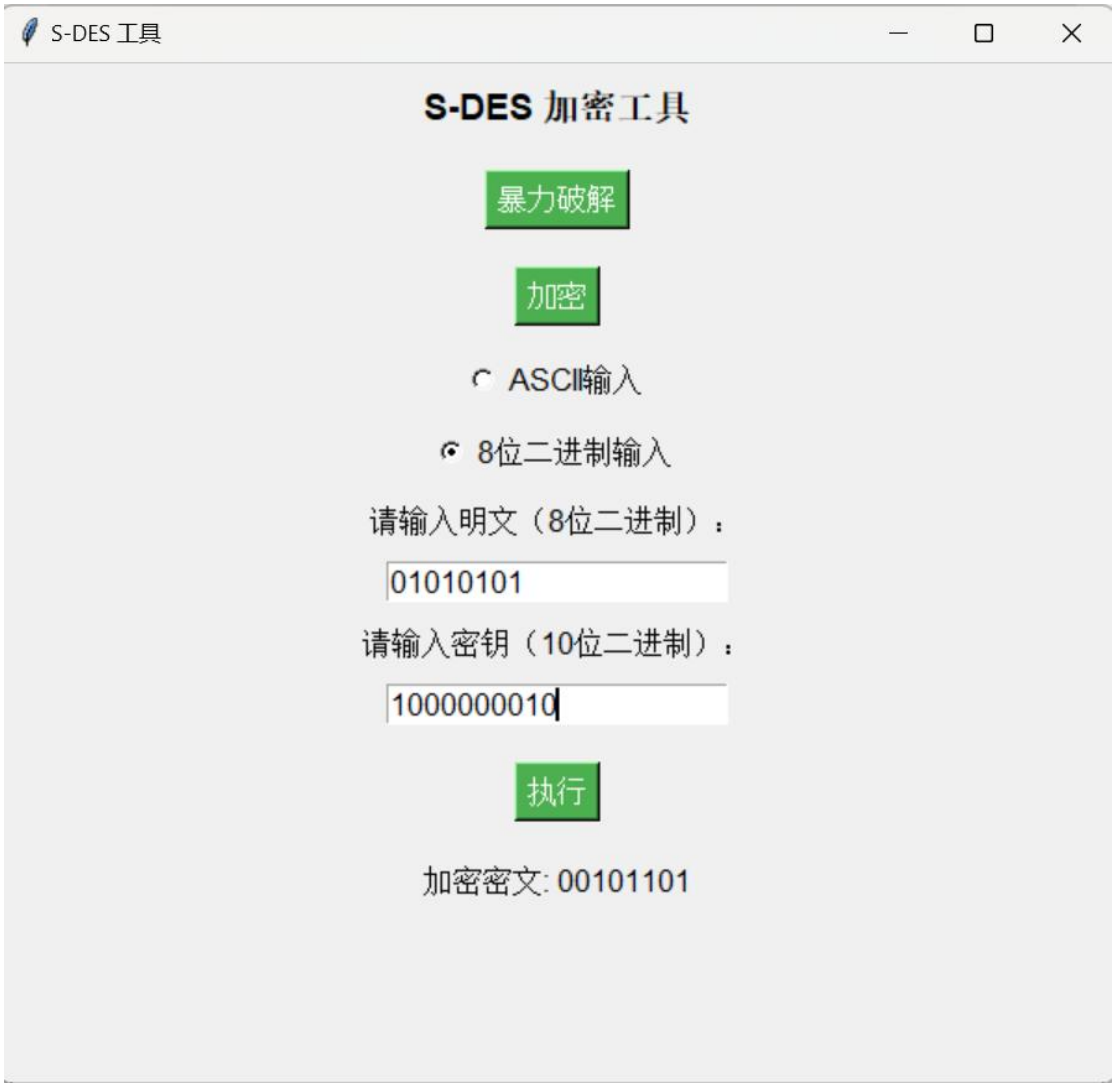
所得密文：00101101



③ 密钥：1000000010

原文：01010101

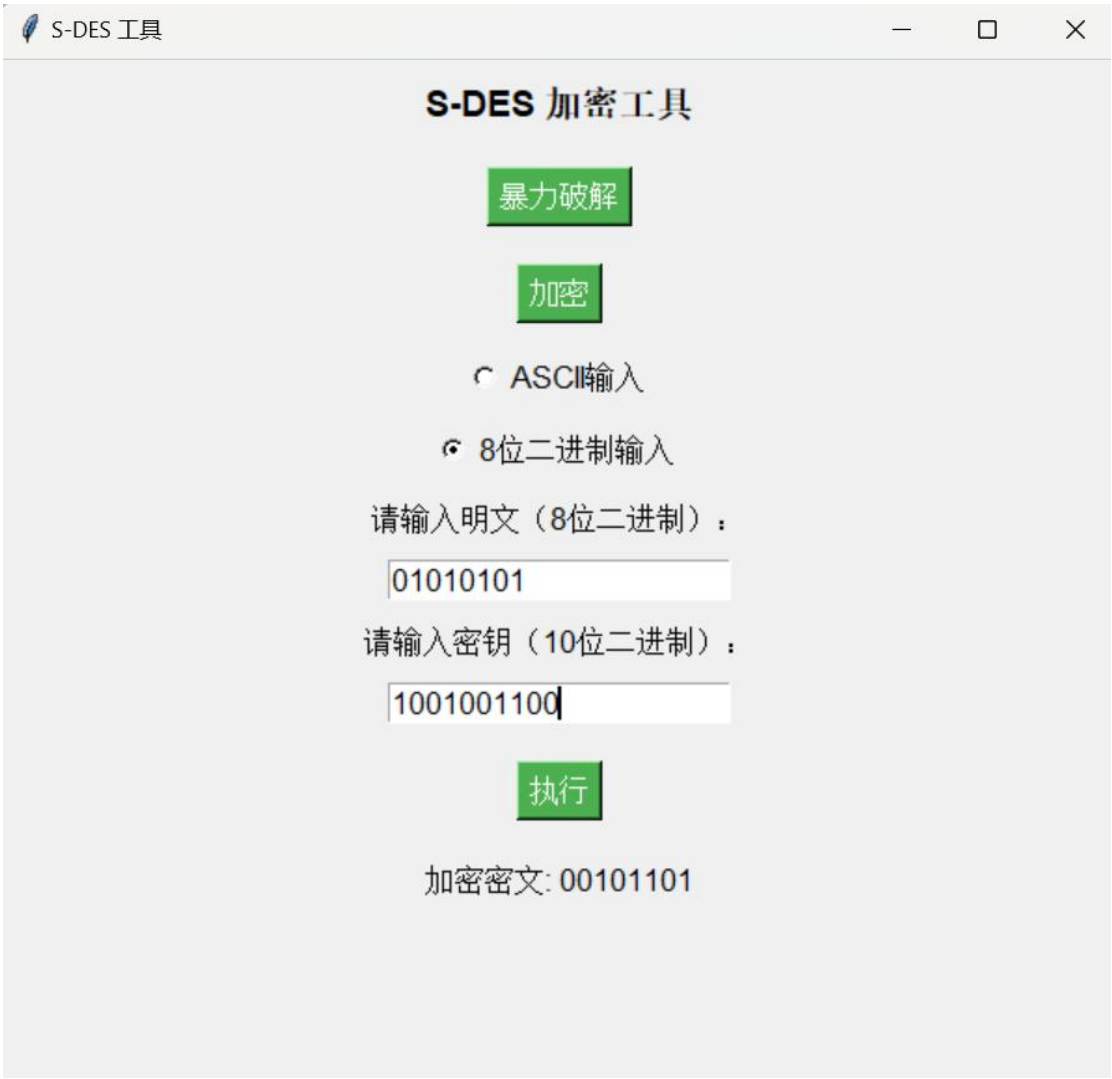
所得密文：00101101



④ 原文：01010101

密钥：1001001100

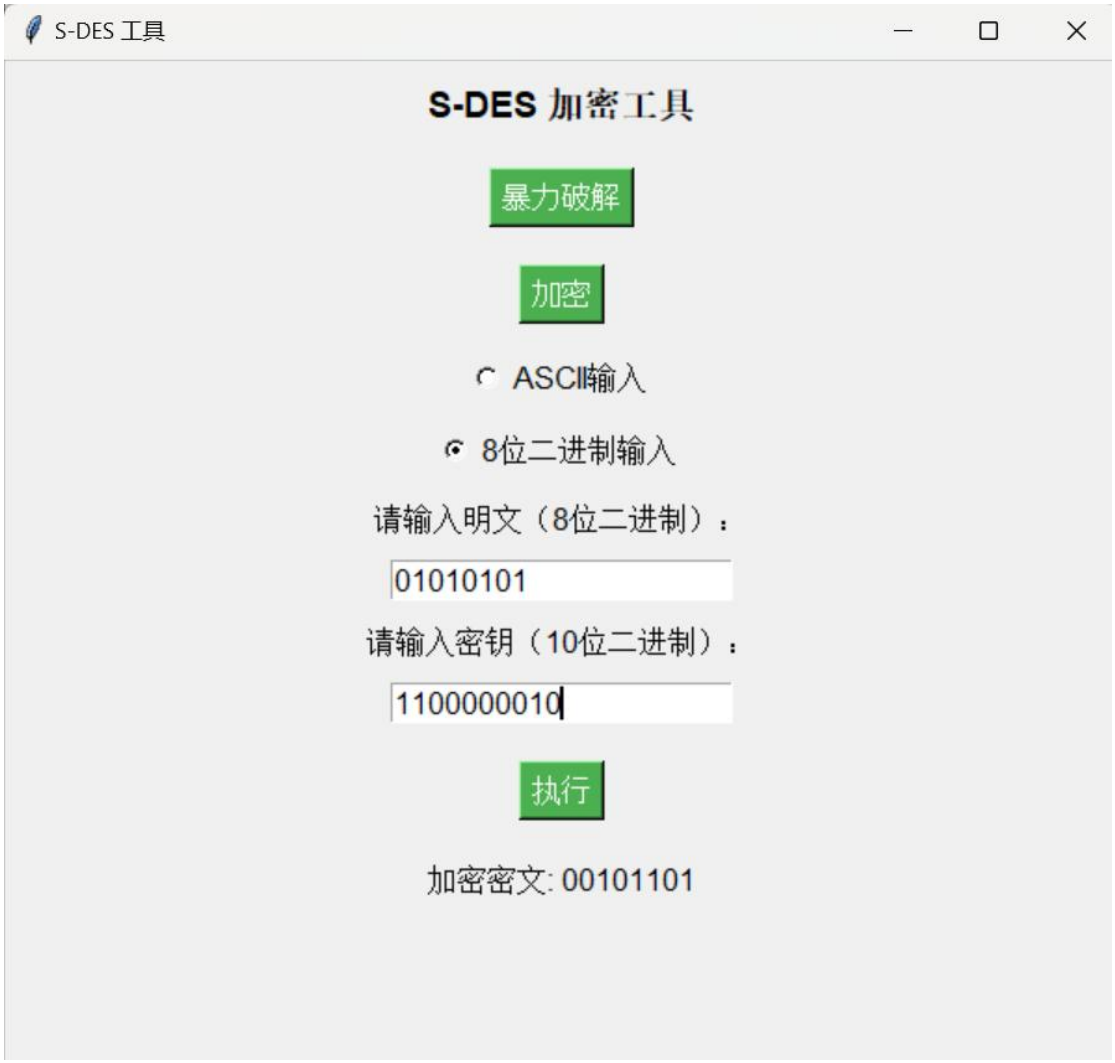
所得密文：00101101



⑤ 密钥：1100000010

原文：01010101

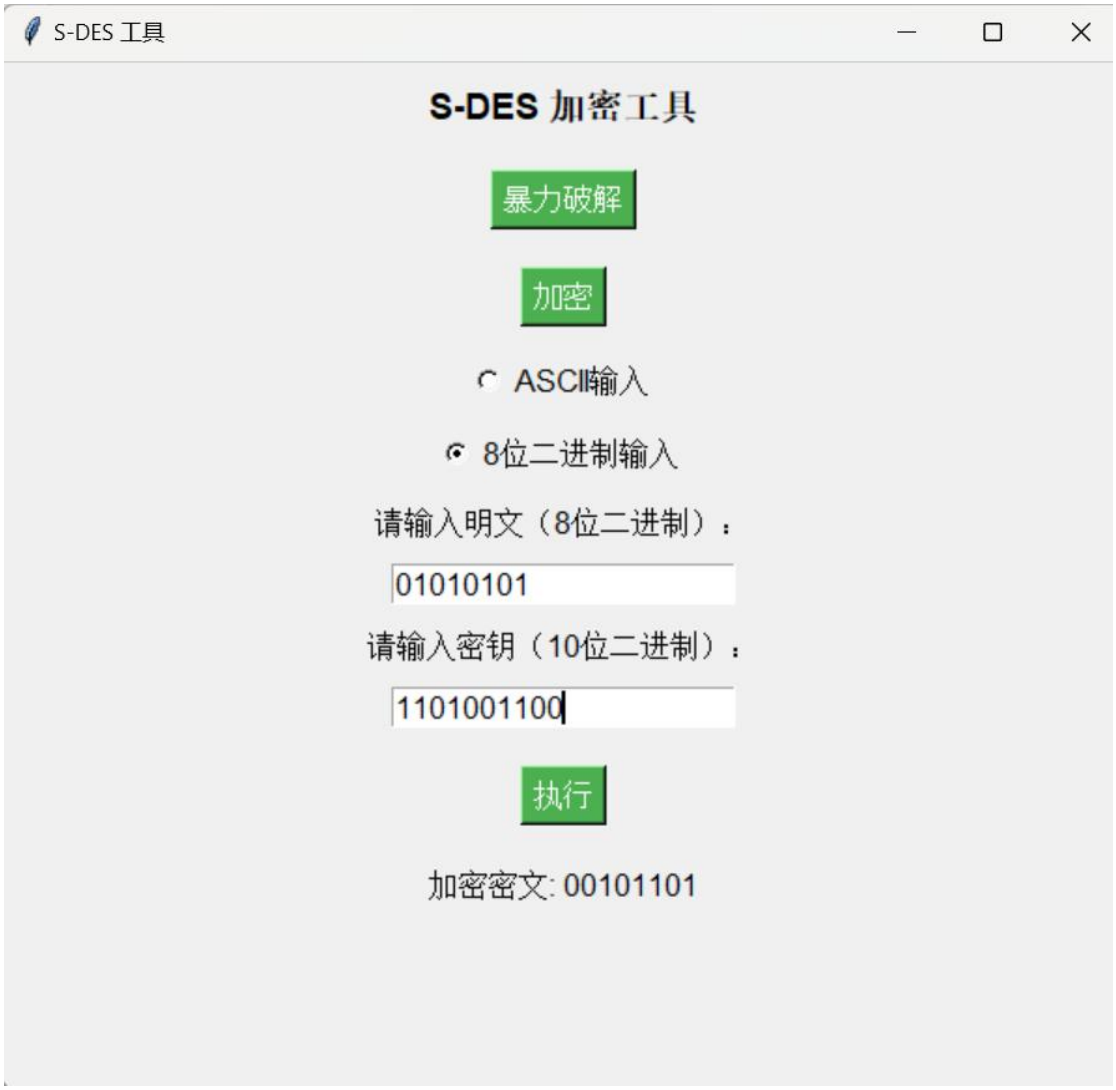
所得密文：00101101



⑥ 密钥：1101001100

原文：01010101

所得密文：00101101



以上六个密钥经测试均能得到相同且符合的明密文对。
在理论上，对于不同的密钥 K 和相同的明文分组 P，应该得到不同的密文 C。这是因为加密算法的设计目的是确保不同密钥产生不同的密文，以增加破解的难度。然而，在一些特殊情况下，可能会出现不同密钥 K 产生相同密文 C 的情况，这通常是由于加密算法的缺陷或弱点所致。在现代密码学中，这种情况被视为严重的安全漏洞，因此加密算法的设计和评估都致力于防止这种情况的发生。

5.3 总结

在本关卡中，我们深入探讨了密码学的基本概念，尤其是密钥多样性和明文-密文对的分析，主要关注以下几个方面：
①密钥多样性：通过实验，我们加深了对加密算法中密钥多样性概念的理解。通常，对于特定的明文-密文对，只有一个唯一的密钥 Key 能生成对应的密文 C，这反映了加密算法的目标，即确保密钥与密文之间的唯一关联，从而保障数据安全。

②密钥选择的影响：我们认识到密钥的选择会显著影响加密结果。不同的密钥会产生不同的密文，而解密时通常需要与之对应的密钥。这突显了在信息安全中，密钥选择和管理的重要性。
③密文关联问题：理论上，不同的密钥 K 和相同的明文分组 P 应生成不同的密文 C。然而，我们也发现，在某些特殊情况下，可能出现不同密钥对应相同密文的情况。这通常源于加密算法的缺陷或漏洞，属于严重的安全隐患。
④密码学的实际应用：该实验进一步深化了我们对密码学在信息安全中的实际应用的理解，强调了其在保护数据机密性和完整性方面的重要性。
⑤实验的反思：通过本次实验，我们反思了密码学的复杂性及其对密钥强度的要求，突显了在算法设计和安全性评估方面的高标准。