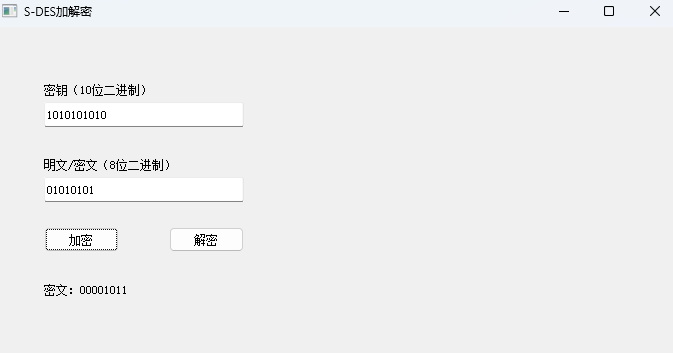
**第1关：基本测试**

明文加密



密文解密



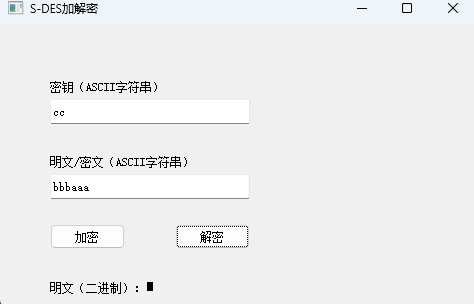
密钥或明文或密文非正确格式



**第2关：交叉测试**

**3.3 第3关：扩展功能**

实用性扩展，密钥，明文，密文可以为ASII编码字符串（有些情况下显示乱码）



**3.4 第4关：暴力破解**

在已知一对明文和密钥时，通过枚举法暴力破解



**3.5 第5关：封闭测试**

在S-DES算法中，对于一个给定的明文和密文对，通常是存在不止一个密钥可以用于加密得到相应的密文。这是因为S-DES算法的密钥空间相对较小，只有1024个可能的密钥。

具体来说，对于给定的明文和密文对（P, C），假设存在两个不同的密钥K1和K2可以将明文P加密为C，即 E(K1, P) = C 和 E(K2, P) = C。这种情况在S-DES算法中是可能发生的，但概率较低。由于密钥的位数较少，可能会出现一些碰撞现象，即不同的密钥对于特定的明文会产生相同的密文。

然而，根据S-DES算法的设计和密钥生成过程，以及S-box的特性，这样的碰撞是相对较少的。对于大多数明文和密文对来说，选择不同的密钥会得到不同的密文。

在扩展到明文空间的情况下，对于给定的明文分组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，与上述情况类似。在S-DES算法中，也有可能发生不同的密钥加密相同的明文分组得到相同的密文分组。但这种情况发生的概率很低，且随着明文分组大小的增加，出现相同密文的可能性会降低。

S-DES算法是一种简化的加密算法，密钥空间相对较小，安全性较低。