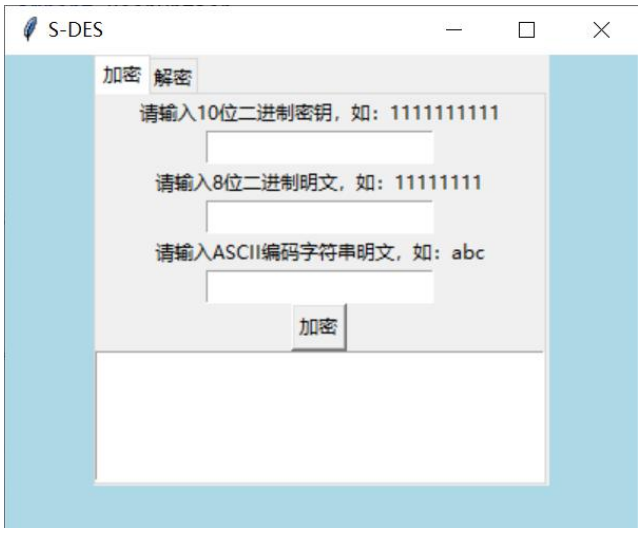
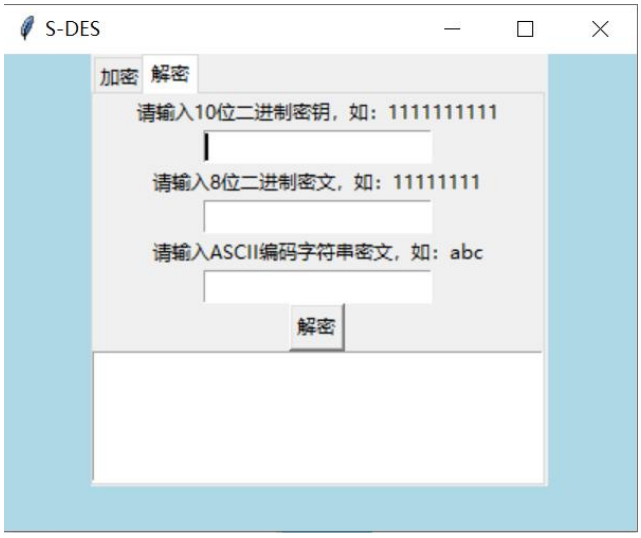
TiMi 小组 1-5 关测试结果

成员：戴静、陈晓阳

第 1 关：基本测试

本小组 GUI 主界面如下：

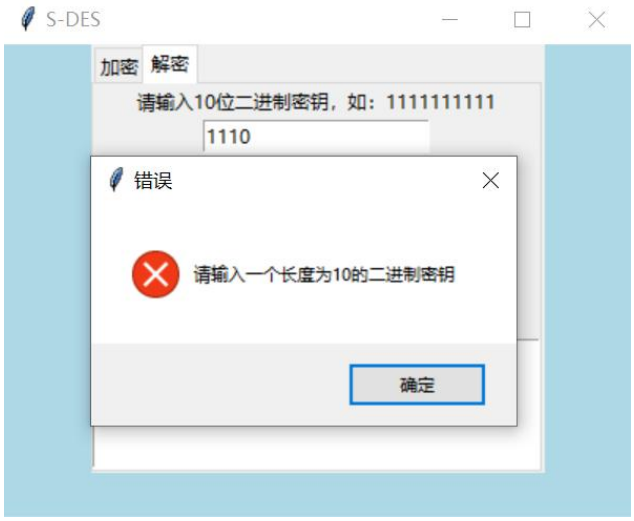


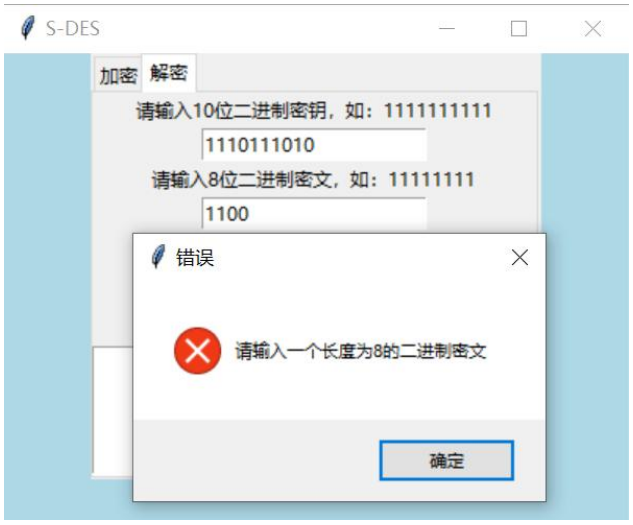


输入部分：加密选项卡输入 10-bit 的密钥、8-bit 的明文（ASCII 编码明文详见第 3 关）；

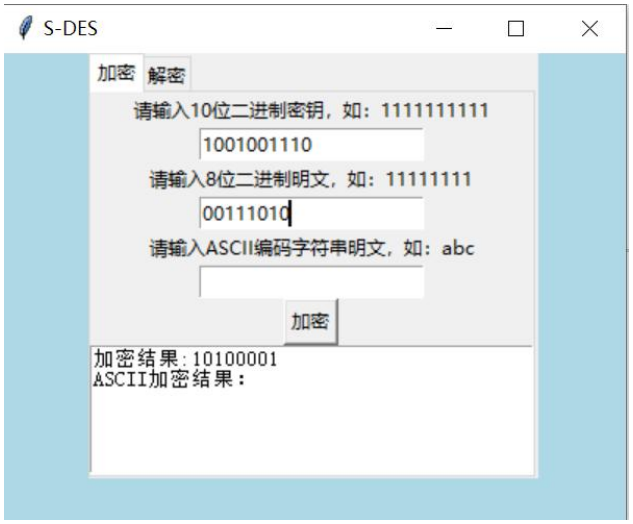
解密选项卡输入加密选项卡输入 10-bit 的密钥、8-bit 的密文（和 ASCII 编码密文）。

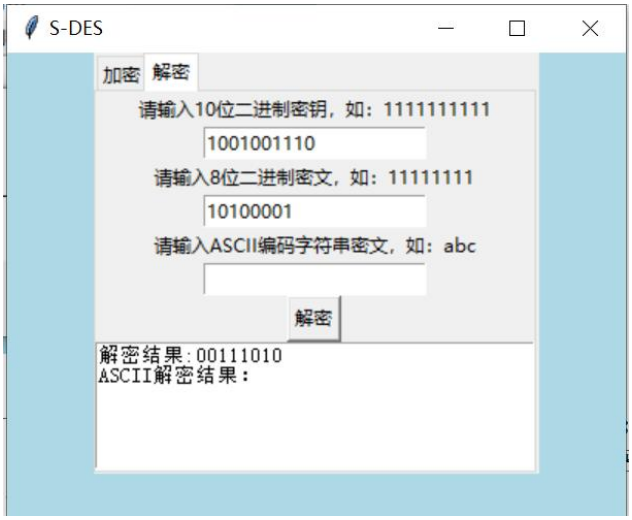
输入错误结果展示：如果输入非 10-bit 的密钥或非 8-bit 的明\密文，将会弹出错误弹窗提示。





输出结果：加密选项卡输入密钥和明文后点击加密，文本框显示加密后的密文；解密选项卡输入密钥和密文后点击解密，文本框显示解密后的明文。





由上两图可见，加密前的明文和解密后的明文保持一致，说明加解密过程无误。第 1 关测试完成。

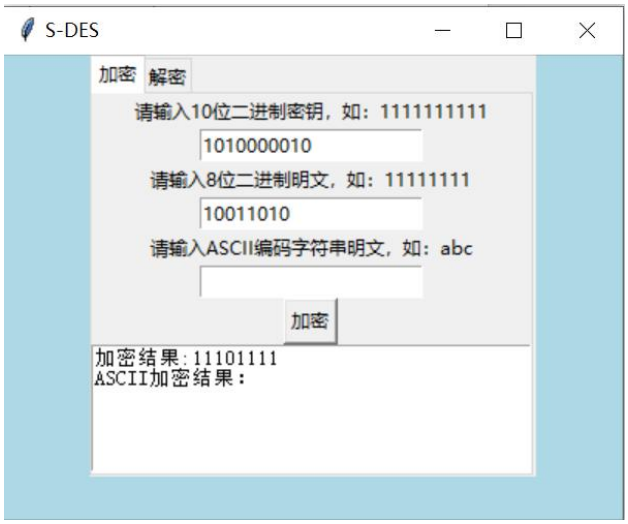
第 2 关：交叉测试

本小组采用“不同小组使用相同的明文 P 和密钥 K 进行加密得到相同的密文 C”的要求进行测试，并与窦一冉组、鲁梦瑶组、唐豪组进行交叉测试。

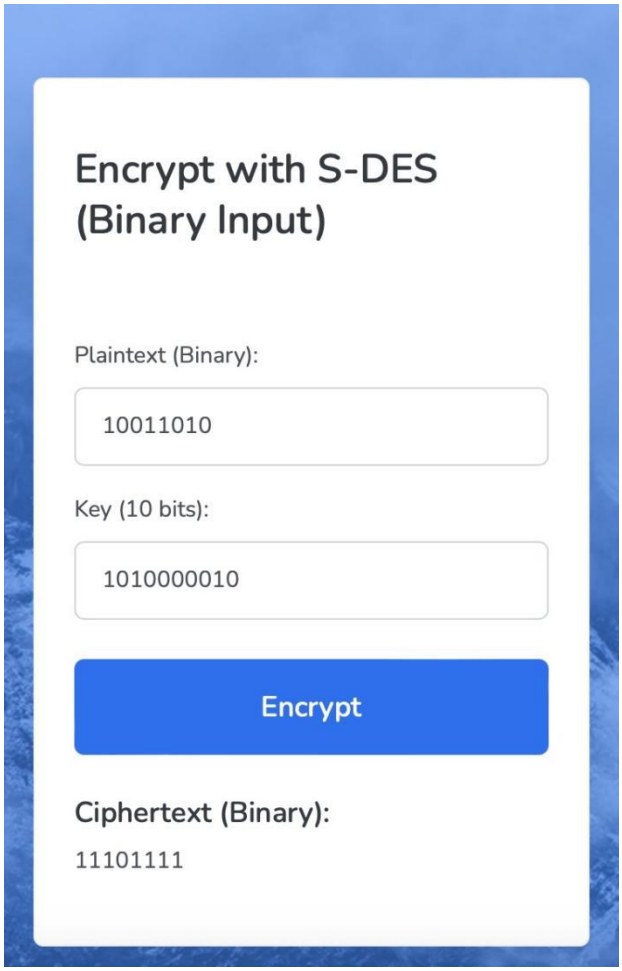
测试明文：10011010

测试密钥：1010000010

本组结果：



窦一冉组结果：



鲁梦瑶组结果：

唐豪组结果：

由上面四组加密结果截图可见，密文均为 11101111，符合交叉测试的通过要求。第 2 关测试完成。

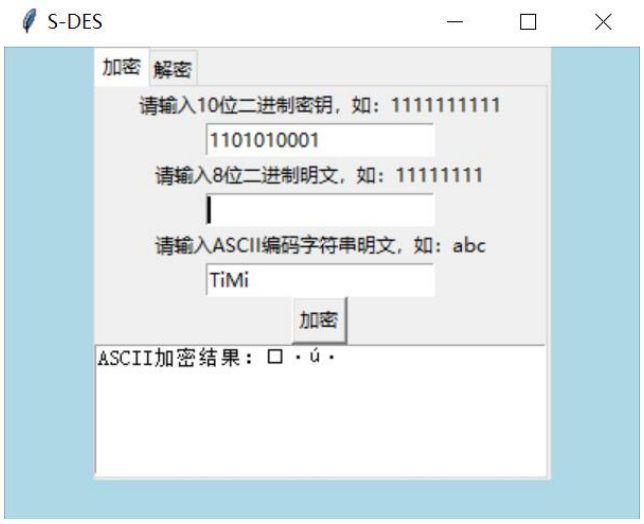
第 3 关：扩展功能

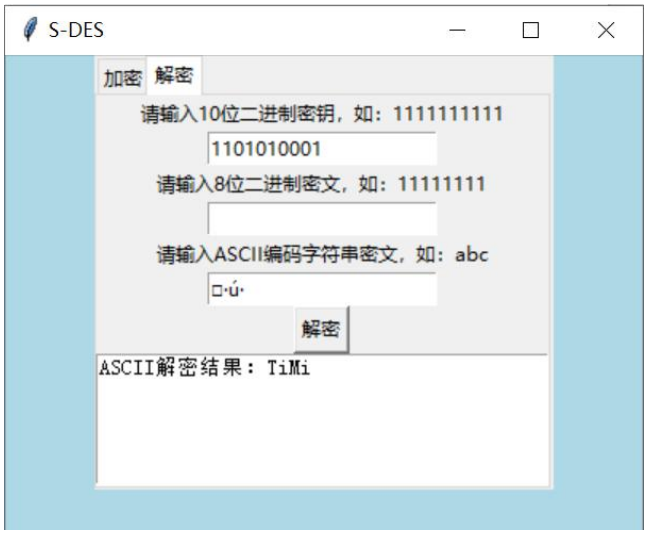
考虑到向实用性扩展，加密算法的数据输入可以是 ASII 编码字符串(分组为 1 Byte)，对应地输出也可以是 ASCII 字符串(很可能是乱码)。本组成功实现了该扩展功能，具体方法如下：将 ASCII 字符串转化为二进制字符串，并以 1 Byte 为一组对该二进制字符串进行循环加密，得到加密后的二进制字符串密文。随后将二进制字符串密文重新转化为 ASCII 字符串输出。解密同理。

输入部分：加密选项卡输入 10-bit 的密钥和 ASCII 编码明文；

解密选项卡输入加密选项卡输入 10-bit 的密钥和 ASCII 编码密文。

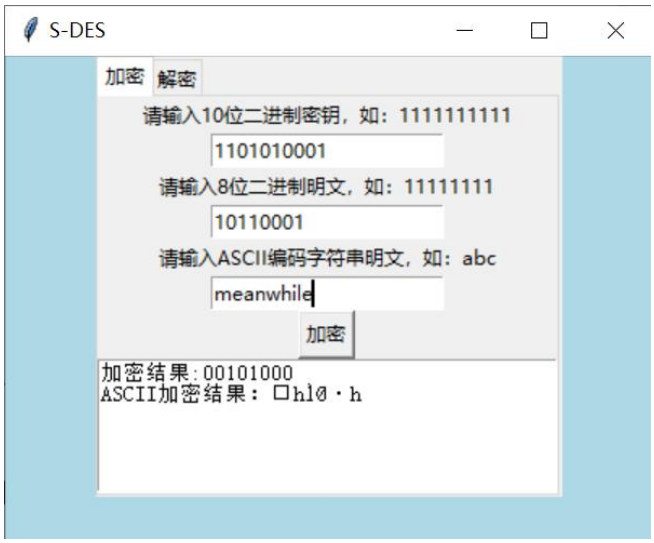
输出结果：加密选项卡输入密钥和 ASCII 明文后点击加密，文本框显示加密后的 ASCII 密文；解密选项卡输入密钥和 ASCII 密文后点击解密，文本框显示解密后的 ASCII 明文。

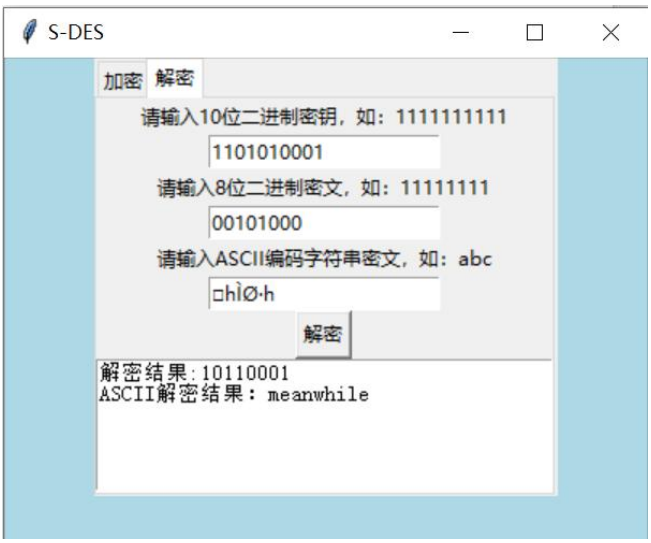




由上两图可见，加密前的明文和解密后的明文保持一致，说明加解密过程无误。第 3 关测试完成。

综合第 1 关和第 3 关，本组的 GUI 实现了普通 8-bit 二进制字符串和 ASCII 编码字符串的同时加\解密，并可以同时显示加\解密结果。效果如下：





第 4 关：暴力破解

本组编写了暴力破解程序，该程序会对一对或多对明密文对进行暴力破解，并统计每对明密文破解的时间，最后计算平均值。暴力破解的过程中，每一条破解过程中的密钥和密文都会被打印；在找到正确的密钥时会进一步打印尝试次数和破解时间。

下两张静态图展示了程序对 3 对使用相同密钥的明、密文对进行暴力破解输入完成的情形和破解完成后的结果。

```
请输入明密文对对数：3
请输入第1对8-bit明文：10100010
请输入第1对8-bit密文：00101100
请输入第2对8-bit明文：10110001
请输入第2对8-bit密文：11000110
请输入第3对8-bit明文：10001111
请输入第3对8-bit密文：00111010
```

```
第1对明密文对找到密钥：1001000110   尝试次数：582,破解时间：0.01810741424560547秒
第2对明密文对找到密钥：0011010100   尝试次数：212,破解时间：0.006891727447509766秒
第3对明密文对找到密钥：1001000110   尝试次数：582,破解时间：0.01683497428894043秒
3对明密文暴力破解找到密钥的平均用时为：0.013944705327351889秒
```

完整破解视频见 Github 链接：https://github.com/jd223344/S-DES

第 4 关测试完成。

第 5 关：封闭测试

根据第 4 关的结果，我们发现三对使用相同密钥 1001000110 的明密文对，在暴力破解时可能找到不同的密钥（如第二对明密文对找到的密钥）。因此，本组编写了相似的新暴力破解程序：对于一组明密文对通过暴力破解的方法找出所有可能的密钥 Key。

我们对第二组明密文对重新进行了暴力破解，结果如下：

```
请输入8-bit明文：10110001
请输入8-bit密文：11000110
找到密钥1:0011010100  累计尝试次数：213，累计破解时间：0.003999948501586914 秒
找到密钥2:0111010100  累计尝试次数：469，累计破解时间：0.008999109268188477 秒
找到密钥3:1001000110  累计尝试次数：583，累计破解时间：0.011998891830444336 秒
找到密钥4:1101000110  累计尝试次数：839，累计破解时间：0.017000675201416016 秒
```

对于该密文对，我们找到了 4 个可能的密钥，且密钥 3 就是关卡 4 中 3 对明密文对原来使用的密钥。

综合第 4 关和第 5 关分析可知，对于随机选择的一个明密文对，可能存在一个或多个密钥 Key。进一步扩展，对应明文空间任意给定的明文分组 Pn，有可能会出现选择不同的密钥 Ki≠Kj 加密得到相同密文 Cn 的情况：只要这些密钥产生的子密钥 k1 和 k2 相同，就可以加密得到相同的密文。

第 5 关测试完成。