测试结果

任务一&&任务三：

任务 1：输入可以是 8bit 的明文数据和 10bit 的密钥，输出是 8bit 的密文。

答：调用 functionalClass 下的 Encrypt 类的 encryptData 函数，输入是一个 int 类型的数组和 10bits 的秘钥 key，进行加密，输出是 lengths 长度为 8 的数组，数组的元素每一位为 0,1。

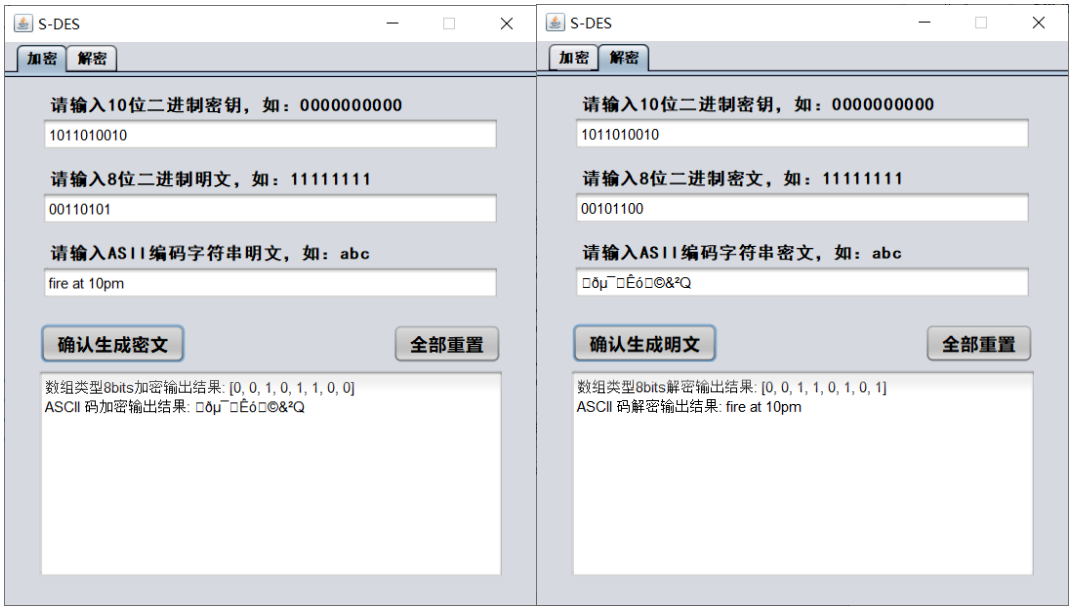
注：数组的每一个元素都是 0,1，在这里我们假定数组的每一个元素代表一个 bit。

任务 3：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)。

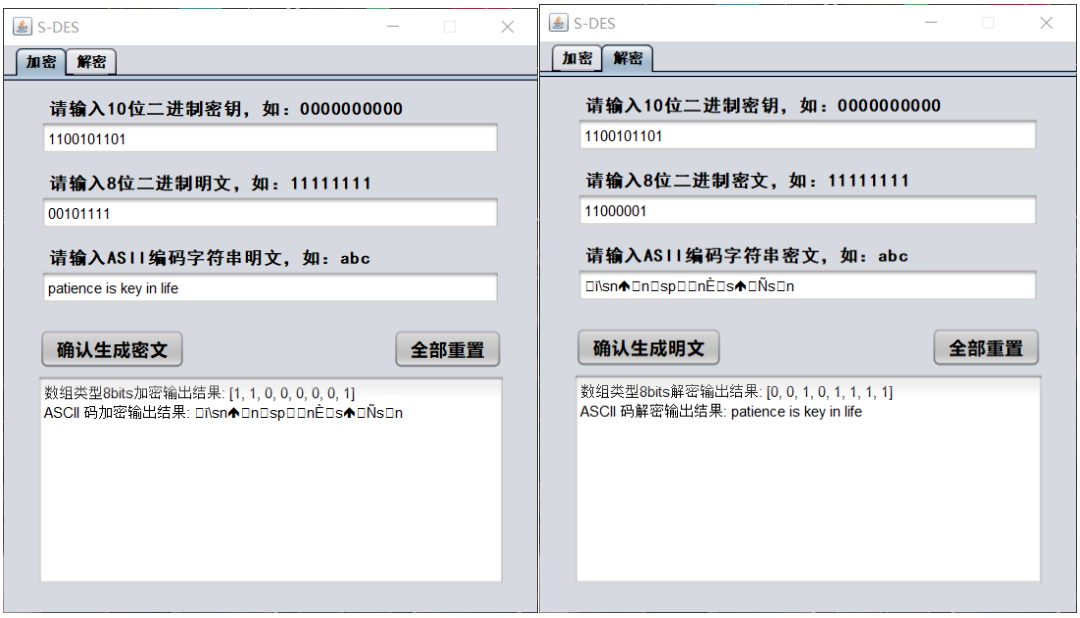
答：调用 functionalClass 下的 Encrypt 类的 encryptASCII 函数，输入是一个 String 类型的 ASCII 编码字符串和 10bits 的秘钥 key。

注：在这里，我们发现，ASCII 码进行加密解密有可能会出现无法显示的情况，也就是一些字符有可能会被加密为控制字符，所以 ASCII 码的加密还是有些状况难以进行正常显示，所以最佳的情形其实是将 ASCII 码进行“01”存储，然后进行解密。

例 1：



例 2：



任务二：

本算法已于多组同学（熊孝宇组、方珩组、朱清扬组）进行共同测验，并检验通过。

任务四：

任务 4：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

答：在项目的 functionalClass 文件夹下的 BruteForceCrack.java 文件中，我展示了五队明文密文对，然后，破解的平均时间在 2ms 左右。运行结果如下：

```
找到秘钥keys: 1010000010
破解时间: 5848 微秒
找到秘钥keys: 1000101000
破解时间: 2095 微秒
找到秘钥keys: 0001110101
破解时间: 399 微秒
找到秘钥keys: 0001101110
破解时间: 416 微秒
找到秘钥keys: 1001000000
破解时间: 1704 微秒
多对明文密文平均破解时间: 2 毫秒
```

任务五：

任务 5：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？

答：是，如在 functionalClass 文件夹下的 ClosedBeta.java 文件展示中的一个明文密文对，就有 2 种密钥对。

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}\ne K_{j}加密得到相同密文 C_n 的情况？

答：会。

运行结果如下：

```
int[] plaintext = {1, 0, 0, 1, 1, 0, 1, 0}; // 已知明文
int[] ciphertext = {1, 1, 1, 0, 1, 1, 1, 1}; // 已知秘文
```

找到以下密钥:

Key=1010000010

Key=1110000010

共找到 2 个密钥。

对于随机选择的一个明密文对，确实有不止一个密钥Key。

在明文空间中存在选择不同的密钥K_i ≠ K_j，但加密得到相同密文C_n的情况。

这些密钥是:

Key=1010000010

Key=1110000010