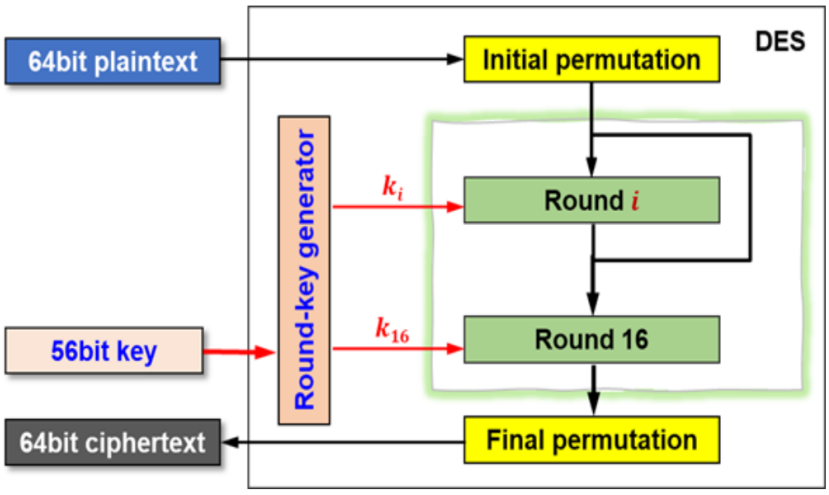
第一关：基本测试

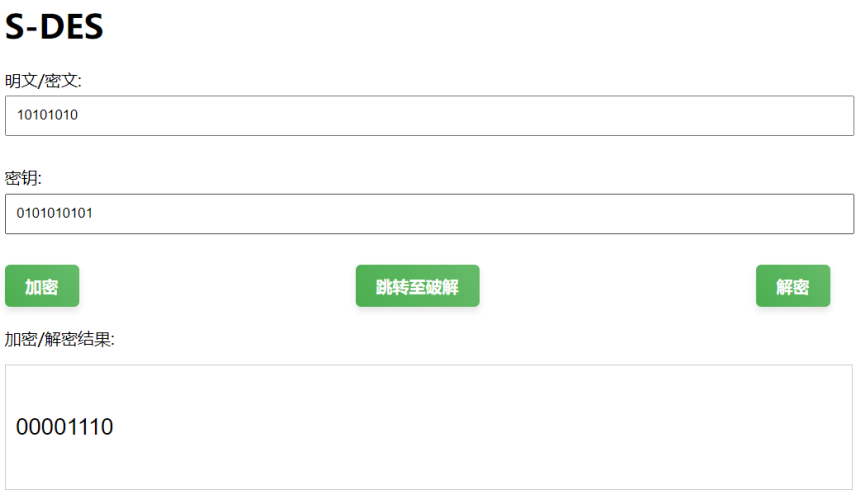
根据 S-DES 算法的编写，提供了 web 页面来实现用户交互，可以输入 8bit 明文/密文和 10bit 密钥来实现加密解密，以下是进行的一些基本测试，加密和解密都测试了几个用例。

加密部分：

明文	密钥	密文
11111111	1111111111	00001111
11111111	0000000000	00010100
11011101	1010101010	11101101
01010101	1010101010	11110001
10101010	0101010101	00001110

加密图片：

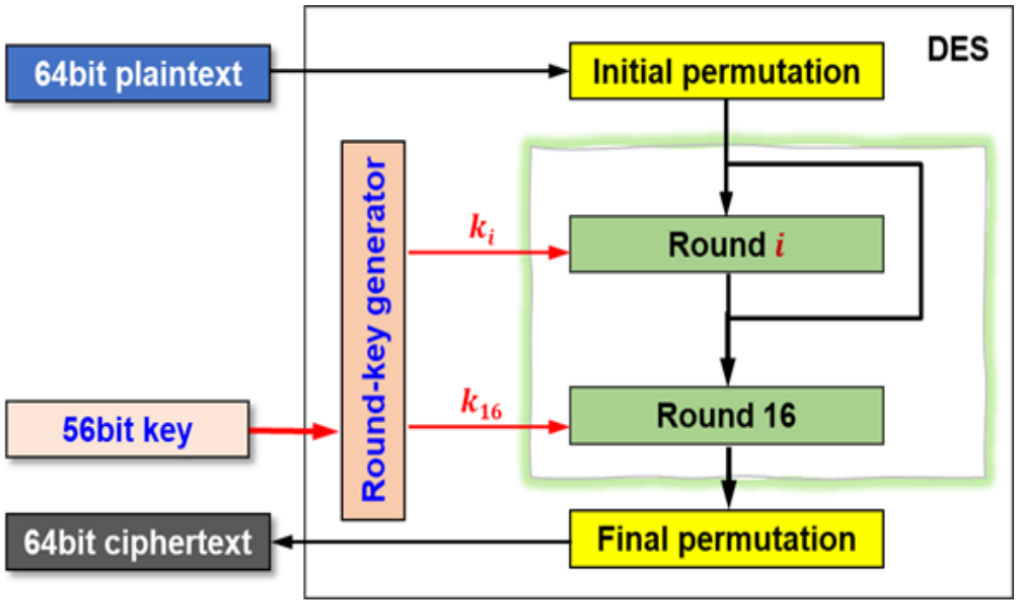


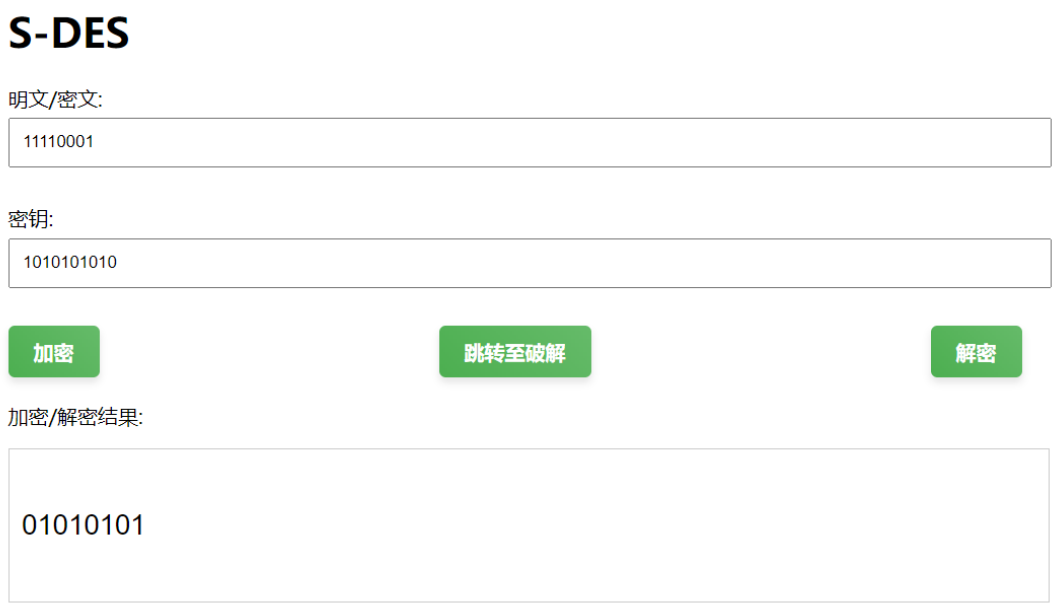


解密部分：

密文	密钥	明文
00001111	1111111111	11111111
00010100	0000000000	11111111
11101101	1010101010	11011101
11110001	1010101010	01010101
00001110	0101010101	10101010

解密图片：

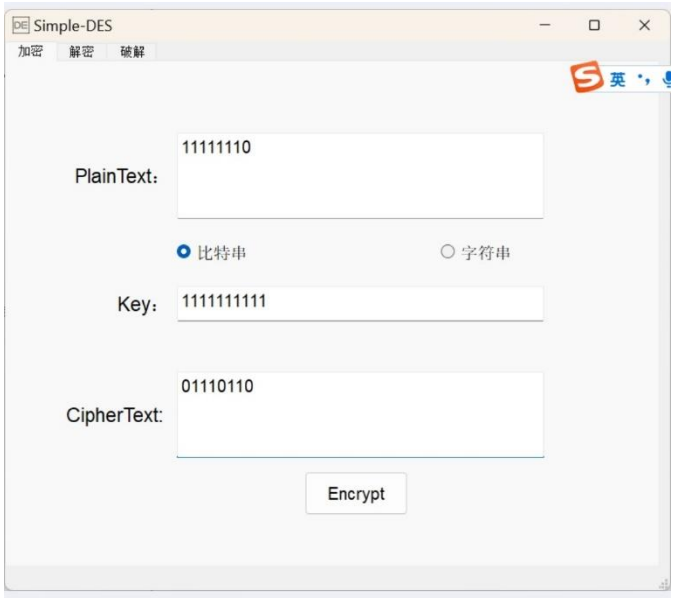




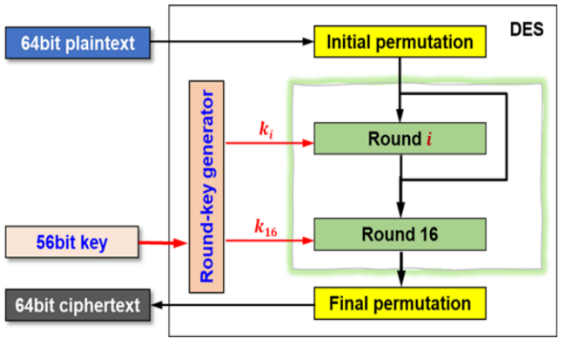
第二关：交叉测试

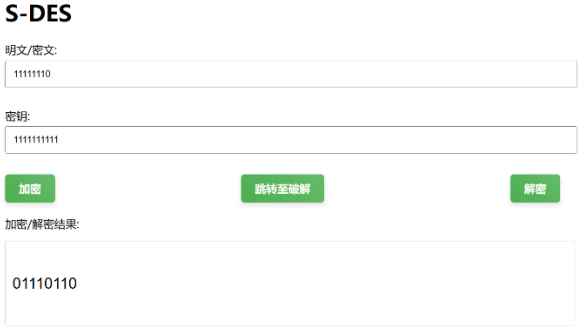
考虑到是算法标准，所有人在编写程序的时候需要使用相同算法流程和转换单元(P-Box、S-Box 等)，以保证算法和程序在异构的系统或平台上都可以正常运行。设有 A 和 B 两组位同学(选择相同的密钥 K)；则 A、B 组同学编写的程序对明文 P 进行加密得到相同的密文 C；或者 B 组同学接收到 A 组程序加密的密文 C，使用 B 组程序进行解密可得到与 A 相同的 P。

A 组同学的结果如下：



B 组同学的结果如下：



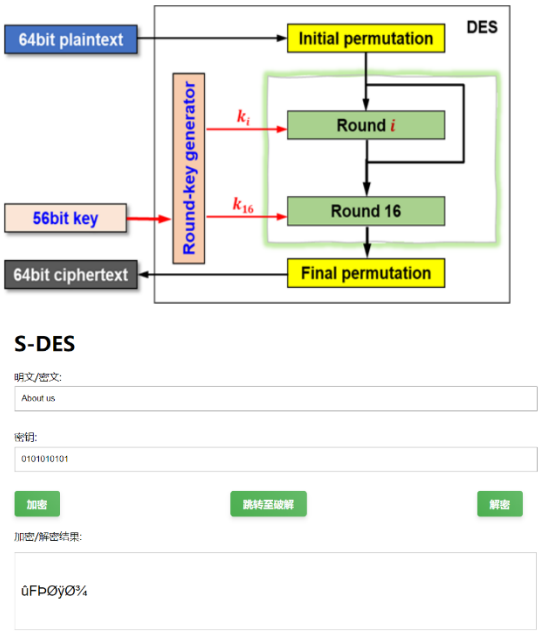


第三关：扩展功能

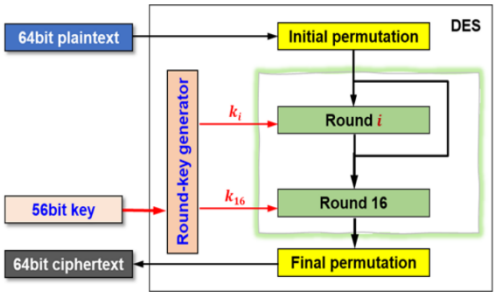
考虑到实用性的拓展，加密/解密算法的输入也可以是 ASCII 字符或者字符串，对应的密文/明文也会是 ASCII 字符或者字符串，但是由于算法的问题最后的输出很可能是乱码字符串。

以下以字符串“About us”，密钥 0101010101 为例子，来测试字符串的加密和解密功能。

字符串加密：

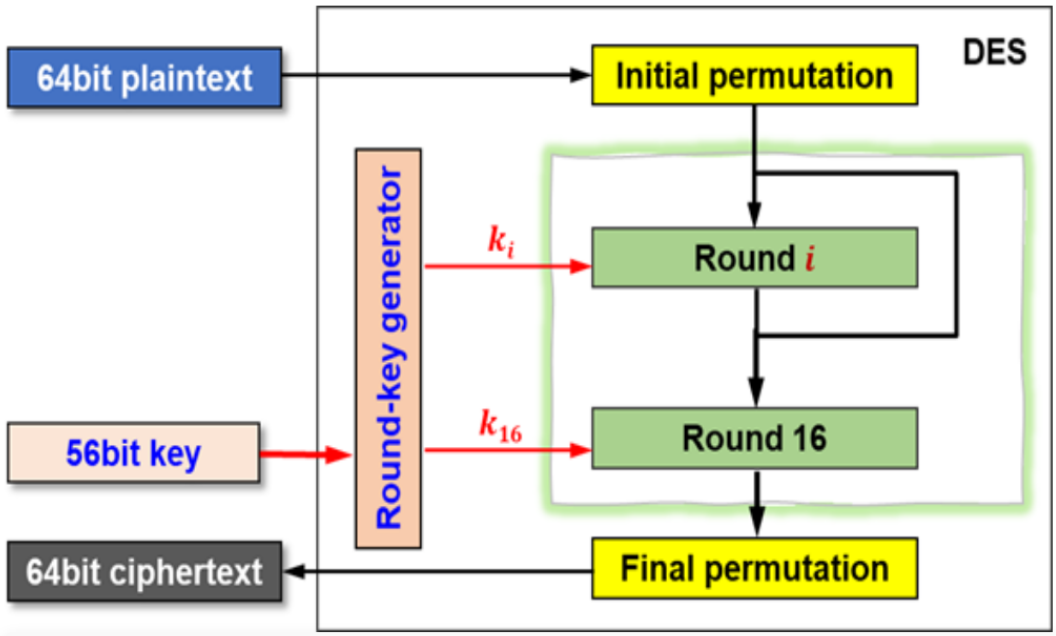


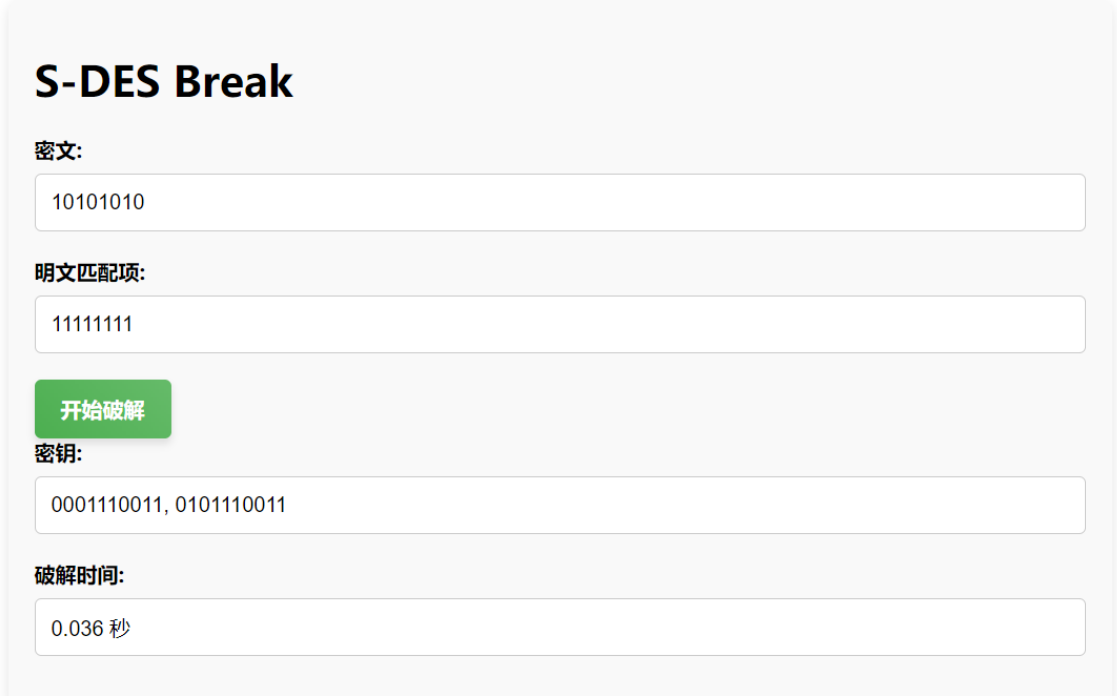
字符串解密：



第四关：暴力破解

程序实现了输入明文密文对来寻找密钥的功能，由于算法的特性一对明文密文对可能存在多个密钥可以被暴力破解出。破解 10101010- 11111111 明文-密文对得到了两个密钥 0001110011 和 0101110011。破解时间为 0.036 秒。





第五关：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？

如明文为 11101101，密文为 11011101 时，可能的密钥有 3 个，分别为 1010101010，1011100000，1110101010，1111100000