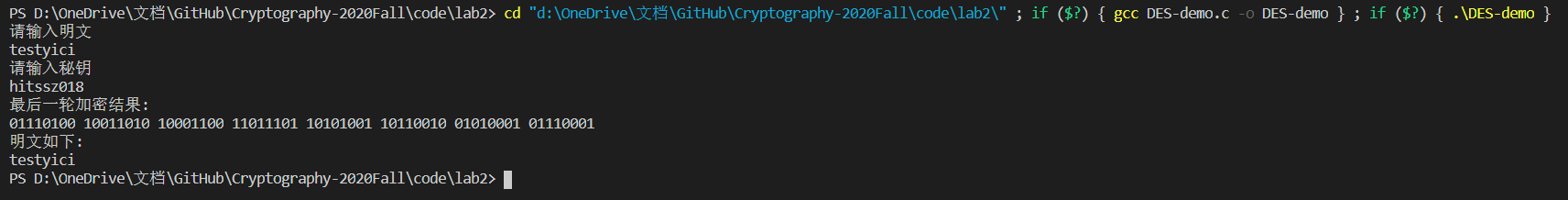
**实验二 DES密码算法**

**姓名：\_\_\_\_\_\_\_\_\_\_胡聪\_\_\_\_\_\_\_\_\_\_\_\_学号：\_\_\_\_\_\_\_\_180110505\_\_\_\_\_\_\_\_\_\_**

1. **运行截图**
2. *截取1组测试结果（密钥为： hitssz018）：内容包括：截图中的内容包括明文，密钥，和对应密钥加密的结果和16轮中每次加密得出的结果，以及解密的密钥和对应解密密钥得出的结果。*

1. **分析一对明文差异只有1位的情况，每轮加密结果的差异。**

**明文：11111111**

**密钥：12345678**

**新密钥：10345678**

**原密钥加密后的各轮结果**

**1 1 1 1 1 1 1 1 0 0 0 0 0 0 0 0 1 1 1 1 1 1 1 1 0 0 0 0 0 0 0 0 1 1 1 0 0 1 0 0 1 1 1 0 1 1 1 1 1 1 0 1 1 0 0 0 0 0 1 0 0 0 1 1**

**1 1 1 0 0 1 0 0 1 1 1 0 1 1 1 1 1 1 0 1 1 0 0 0 0 0 1 0 0 0 1 1 0 1 0 1 0 0 0 1 0 0 1 0 1 0 1 0 0 0 1 1 1 1 1 0 0 0 0 1 0 1 0 1**

**0 1 0 1 0 0 0 1 0 0 1 0 1 0 1 0 0 0 1 1 1 1 1 0 0 0 0 1 0 1 0 1 1 0 0 1 1 0 1 1 1 1 0 0 1 0 0 0 0 0 0 1 1 1 0 0 0 0 0 1 0 0 0 1**

**1 0 0 1 1 0 1 1 1 1 0 0 1 0 0 0 0 0 0 1 1 1 0 0 0 0 0 1 0 0 0 1 0 1 1 0 0 1 1 0 0 1 1 0 1 0 0 0 0 0 1 0 0 0 0 1 1 1 1 0 1 1 1 1**

**0 1 1 0 0 1 1 0 0 1 1 0 1 0 0 0 0 0 1 0 0 0 0 1 1 1 1 0 1 1 1 1 0 0 1 0 1 1 0 1 0 1 0 0 1 1 0 0 1 0 0 1 0 0 1 1 0 0 1 1 0 0 1 1**

**0 0 1 0 1 1 0 1 0 1 0 0 1 1 0 0 1 0 0 1 0 0 1 1 0 0 1 1 0 0 1 1 1 0 1 0 1 1 0 1 0 0 1 0 0 1 1 0 1 1 1 1 1 1 1 1 1 1 0 0 1 1 1 1**

**1 0 1 0 1 1 0 1 0 0 1 0 0 1 1 0 1 1 1 1 1 1 1 1 1 1 0 0 1 1 1 1 0 1 1 1 0 1 1 0 1 1 1 0 0 1 1 0 1 1 0 0 0 0 0 1 1 0 1 0 1 0 1 1**

**0 1 1 1 0 1 1 0 1 1 1 0 0 1 1 0 1 1 0 0 0 0 0 1 1 0 1 0 1 0 1 1 0 0 1 1 1 0 1 1 1 1 0 1 0 0 0 1 0 1 0 1 0 0 0 0 1 1 0 0 0 1 0 0**

**0 0 1 1 1 0 1 1 1 1 0 1 0 0 0 1 0 1 0 1 0 0 0 0 1 1 0 0 0 1 0 0 1 0 0 0 0 1 1 1 1 1 0 1 0 1 1 0 0 1 0 1 1 1 0 0 1 1 1 1 1 1 0 1**

**1 0 0 0 0 1 1 1 1 1 0 1 0 1 1 0 0 1 0 1 1 1 0 0 1 1 1 1 1 1 0 1 1 0 1 1 1 1 0 0 0 1 1 0 0 0 0 1 0 0 0 1 0 1 0 0 0 1 0 1 0 1 0 1**

**1 0 1 1 1 1 0 0 0 1 1 0 0 0 0 1 0 0 0 1 0 1 0 0 0 1 0 1 0 1 0 1 1 1 1 1 1 0 1 1 1 1 1 0 1 0 0 1 0 1 1 1 0 0 1 0 1 1 1 0 0 0 0 1**

**1 1 1 1 1 0 1 1 1 1 1 0 1 0 0 1 0 1 1 1 0 0 1 0 1 1 1 0 0 0 0 1 0 1 1 1 1 1 0 0 0 1 0 0 0 0 1 1 1 0 0 0 0 1 0 1 0 0 0 1 1 0 0 0**

**0 1 1 1 1 1 0 0 0 1 0 0 0 0 1 1 1 0 0 0 0 1 0 1 0 0 0 1 1 0 0 0 0 0 0 0 0 1 1 1 0 0 0 1 0 0 1 0 1 1 0 0 1 1 0 0 1 0 0 0 1 0 1 0**

**0 0 0 0 0 1 1 1 0 0 0 1 0 0 1 0 1 1 0 0 1 1 0 0 1 0 0 0 1 0 1 0 1 0 0 1 1 1 0 1 0 1 1 0 1 0 0 1 0 0 1 1 1 1 1 1 1 1 1 1 1 0 0 1**

**1 0 0 1 1 1 0 1 0 1 1 0 1 0 0 1 0 0 1 1 1 1 1 1 1 1 1 1 1 0 0 1 0 0 1 1 1 1 0 0 0 0 1 0 1 1 1 1 0 0 0 0 1 0 0 1 0 0 1 0 1 0 0 0**

**0 0 1 1 1 1 0 0 0 0 1 0 1 1 1 1 0 0 0 0 1 0 0 1 0 0 1 0 1 0 0 0 0 1 1 1 0 1 1 1 1 1 0 0 1 1 0 1 1 1 0 0 0 1 0 0 1 1 1 1 1 0 0 1**

**新密钥加密后的各轮结果**

**1 1 1 1 1 1 1 1 0 0 0 0 0 0 0 0 1 1 1 1 1 1 1 1 0 0 0 0 0 0 0 0 1 1 1 0 0 1 0 0 0 1 1 0 1 1 1 1 0 1 0 1 1 0 1 0 0 0 1 0 0 0 0 1**

**1 1 1 0 0 1 0 0 0 1 1 0 1 1 1 1 0 1 0 1 1 0 1 0 0 0 1 0 0 0 0 1 0 0 0 1 0 0 0 0 0 1 0 0 1 0 0 1 0 1 1 0 0 1 1 0 1 0 1 0 1 0 0 1**

**0 0 0 1 0 0 0 0 0 1 0 0 1 0 0 1 0 1 1 0 0 1 1 0 1 0 1 0 1 0 0 1 0 1 0 1 1 0 1 0 0 0 0 0 0 0 1 0 1 0 0 0 1 1 1 0 0 1 1 0 1 0 1 1**

**0 1 0 1 1 0 1 0 0 0 0 0 0 0 1 0 1 0 0 0 1 1 1 0 0 1 1 0 1 0 1 1 0 1 0 1 1 0 1 1 0 1 0 0 0 0 0 1 0 0 1 1 0 1 1 1 0 1 1 0 0 0 1 1**

**0 1 0 1 1 0 1 1 0 1 0 0 0 0 0 1 0 0 1 1 0 1 1 1 0 1 1 0 0 0 1 1 1 0 1 1 1 0 0 0 0 1 1 1 1 1 0 1 0 1 1 0 0 0 0 0 0 0 1 0 0 1 0 1**

**1 0 1 1 1 0 0 0 0 1 1 1 1 1 0 1 0 1 1 0 0 0 0 0 0 0 1 0 0 1 0 1 0 1 1 1 1 0 1 1 0 0 0 0 1 1 1 0 1 0 0 1 1 1 1 1 1 1 1 1 1 1 0 1**

**0 1 1 1 1 0 1 1 0 0 0 0 1 1 1 0 1 0 0 1 1 1 1 1 1 1 1 1 1 1 0 1 0 0 0 0 1 0 1 1 1 0 0 0 1 1 1 0 0 0 1 0 0 0 0 0 0 1 0 0 1 0 1 1**

**0 0 0 0 1 0 1 1 1 0 0 0 1 1 1 0 0 0 1 0 0 0 0 0 0 1 0 0 1 0 1 1 1 0 1 0 1 1 0 0 0 1 0 0 0 0 0 1 0 1 0 1 0 0 1 1 1 1 1 1 0 0 0 0**

**1 0 1 0 1 1 0 0 0 1 0 0 0 0 0 1 0 1 0 1 0 0 1 1 1 1 1 1 0 0 0 0 0 1 1 1 1 1 0 0 1 1 1 1 1 1 1 1 1 1 1 1 0 1 1 0 0 1 1 0 0 1 0 1**

**0 1 1 1 1 1 0 0 1 1 1 1 1 1 1 1 1 1 1 1 0 1 1 0 0 1 1 0 0 1 0 1 0 0 1 1 0 1 1 1 0 1 1 1 0 1 0 0 1 1 1 1 0 1 0 0 0 1 1 1 1 0 0 1**

**0 0 1 1 0 1 1 1 0 1 1 1 0 1 0 0 1 1 1 1 0 1 0 0 0 1 1 1 1 0 0 1 0 1 1 0 1 0 1 0 0 1 0 0 1 0 1 1 1 0 0 1 0 1 0 0 0 1 1 0 1 1 0 1**

**0 1 1 0 1 0 1 0 0 1 0 0 1 0 1 1 1 0 0 1 0 1 0 0 0 1 1 0 1 1 0 1 1 1 1 1 0 0 1 0 1 0 1 1 0 1 0 1 0 1 0 0 0 1 0 0 0 1 1 1 0 0 0 1**

**1 1 1 1 0 0 1 0 1 0 1 1 0 1 0 1 0 1 0 0 0 1 0 0 0 1 1 1 0 0 0 1 0 0 1 0 1 0 1 0 0 1 0 1 1 0 1 1 1 0 1 1 0 1 1 0 1 0 1 0 0 0 1 1**

**0 0 1 0 1 0 1 0 0 1 0 1 1 0 1 1 1 0 1 1 0 1 1 0 1 0 1 0 0 0 1 1 1 0 1 1 0 1 0 0 0 0 0 1 0 0 0 1 0 0 0 0 1 0 1 1 0 1 1 0 0 0 0 0**

**1 0 1 1 0 1 0 0 0 0 0 1 0 0 0 1 0 0 0 0 1 0 1 1 0 1 1 0 0 0 0 0 1 0 1 1 0 1 1 0 0 0 1 1 0 0 1 0 1 0 1 0 0 0 1 1 1 0 0 0 0 0 0 0**

**1 0 1 1 0 1 1 0 0 0 1 1 0 0 1 0 1 0 1 0 0 0 1 1 1 0 0 0 0 0 0 0 0 1 1 0 1 0 1 0 0 0 0 0 1 1 0 1 0 1 1 1 1 1 1 1 0 1 0 1 1 0 0 1**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **加密轮数** | **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** |
| **相差bit** | **4** | **18** | **29** | **29** | **30** | **28** | **28** | **28** |
| **加密轮数** | **9** | **10** | **11** | **12** | **13** | **14** | **15** | **16** |
| **相差bit** | **29** | **30** | **27** | **31** | **32** | **29** | **28** | **28** |

1. **总结**

通过本次实验，我明白了DES的主要弱点，一个是密钥容量不足，难以提供足够的安全性，同时DES的密钥长度可能太小，迭代次数较小，这些弱点使得DES存在较大的保密风险。通过本次实验对于信息安全有了更加深刻的认识，同时通过编程实现了DES密码算法，收获很大。