**2021 密码实验班 应用密码学实验报告内容**

|  |
| --- |
| **实验报告一、DES密码实现**   1. DES明文扩展（32bit扩展到64bit） 2. DES的8个S盒运算实现 3. DES子密钥生成算法实现 4. 调用实验二中1-3的程序，实现DES加密解密 |
| **实验报告二、AES密码实现**   1. AES列混合实现 2. AES子密钥生成算法 3. AES加密的实现（可调用S盒） |
| **实验报告三、公钥算法实现**   1. RSA加解密 2. ElGamal加解密 3. Diffie-Hellman密钥交换协议实现 |
| **实验报告四、Hash函数实现**   1. SHA-1的实现（可调用python中相关部件） 2. MD5的实现（可调用python中相关部件） |

**注：每个报告内容，单独一个word文档。**