1. 介绍一种密码体制，除上课重点介绍的以外，即除DES，AES，MD5，SHA，RSA和Elgamal以外。
2. 介绍内容包括但不限于：密码算法（加密，解密，密钥生成或签名、验证等）、参数说明（如分组大小，密钥长度等）、密码原理（如解密对加密的正确性，验证对签名的正确性等）、约束或限制（如弱密钥等）、安全性说明（不需要严格证明，只是大致说明安全强度，攻击的计算复杂性）。
3. 可以有简单的数字例子帮助演示。
4. 列出参考文献。
5. 全文无字数要求。
6. 文件名以学号||姓名表示，学号在前，学号用全部号码，不要只写后几位。
7. 十八周之前都可以（不包括十八周），后面是考试周，你们也没有时间撰写了。