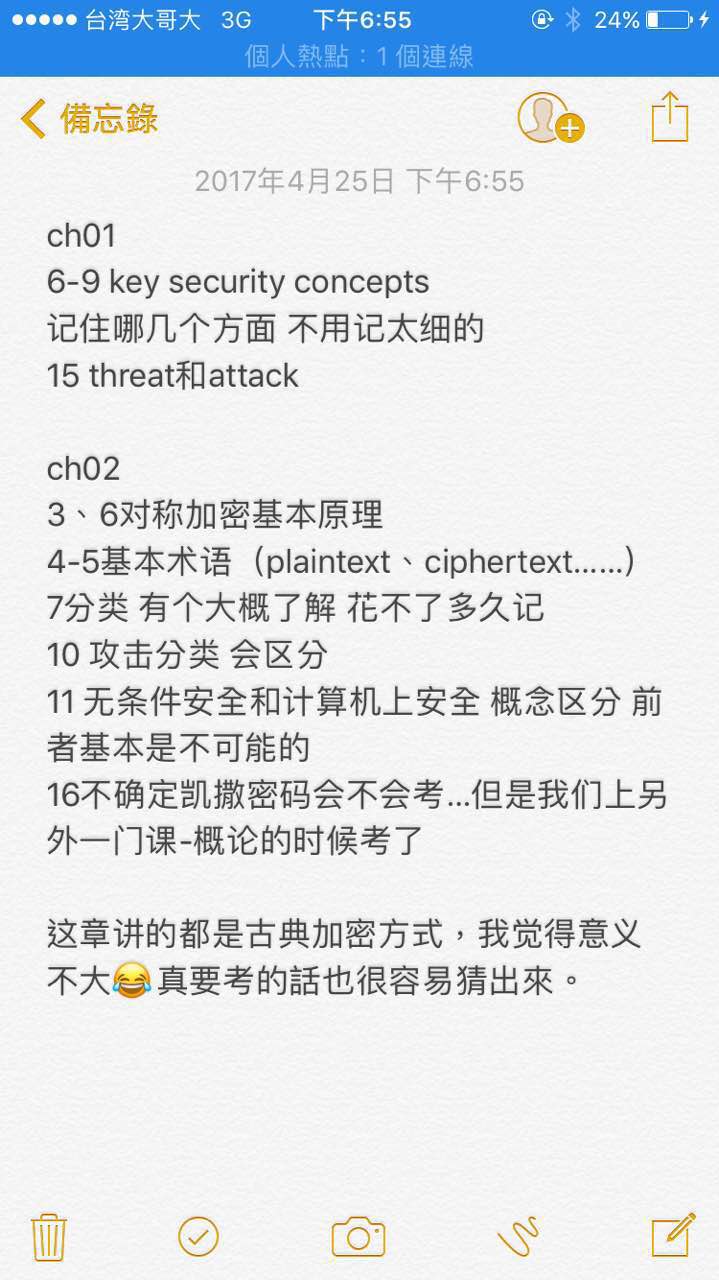
gfp gf2^n 写例子

选择题 des 演算法熟悉

作业 古典演算法 加解密

block cipher mod



ch01是ppt右下角有數字標著

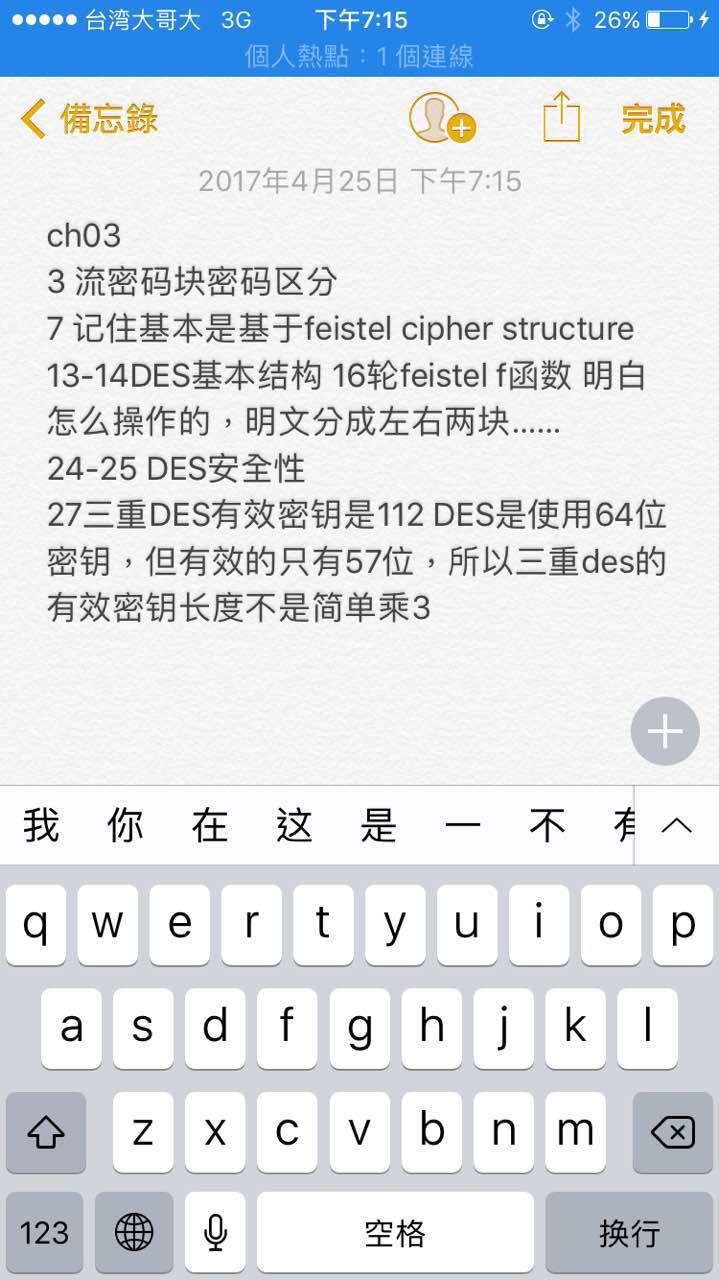
ch02就是pdf阅读器显示的页码了

搞明白DES原理 模运算

加上GCD算法 45页的GF

第五章讲的就是AES 记住有三种密钥长度 然后明白他的原理

第六章 知道这四个块加密模式ECB CBC OFB CFB然后知道区别 鸽笼原理



1 加密算法

对称加密 symmetric ciphers

非对称加密 asymmetric encryption

哈希函数 散列函数 hash functions

2 互相信任

秘钥管理和分发

用户认证

Key security concepts CIA triad

1. Confidentiality
2. Integrity
3. Availability
4. Authenticity
5. Accountability