## 2.28

加密和解密：安全信道

取模运算

一次一密是无条件安全，为什么不方便使用？因为OTP不方便，解密文件和传输文件同个大小，在传输过程极不实用。

密钥长度和明文一样长，不实用

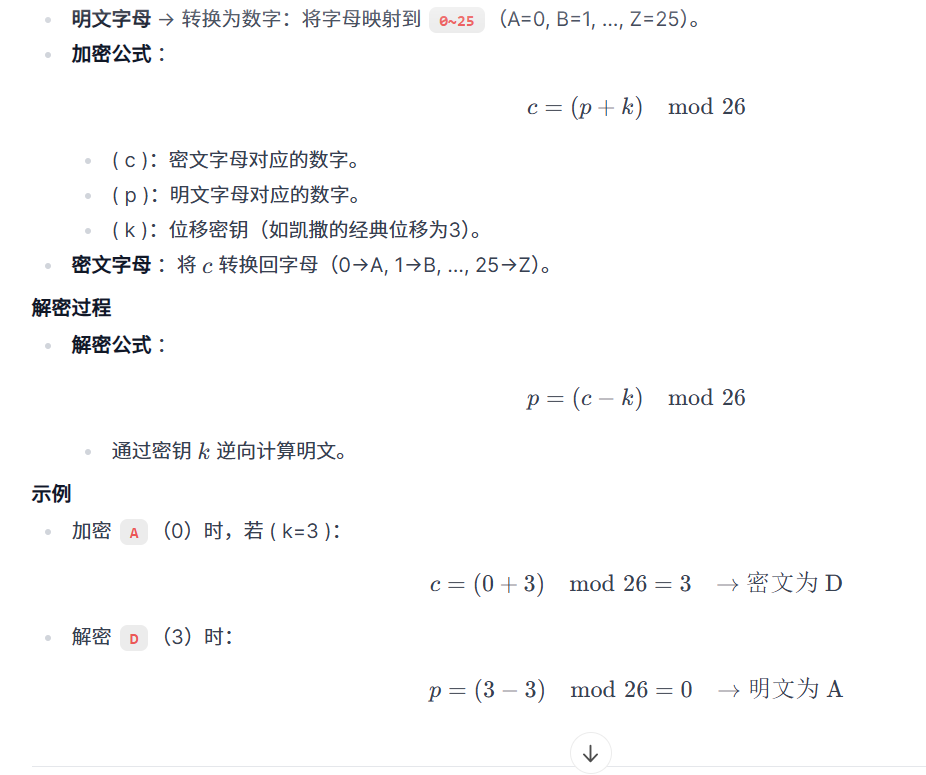
计算安全

实用流密钥通信模型

Si不是真实际数，而是伪的，由K代产生。由发生器随机产生的我觉得是实用的，密钥长度不需要很大，可以进行复杂加密

1000个视频，为2的1000-1次方

2.用模算术描述Caesar加密算法.



为什么加密算法应该公开？

公开的加密算法可以受到外界的检测和尝试破解，如果加密算法被破解，它就能得到修改和完善，这样反反复复接受外界挑战，直到最后，这个加密算法才有很高的安全性和可靠性。

算法保密无法保证长期安全。公开算法后，经过全球专家的审查和攻击测试，能暴露漏洞并改进。

一次一密(OTP)是无条件安全的，但它为什么不实用？

因为它的解密文件和传输文件是同个大小，在传输过程非常不方便，不方便解密，实用性不高

密钥管理复杂度，密钥存储需物理隔离，防止泄露

## 3.14.2025

CBC加密和电子密码本加密word文档





