Atitit 安全法基础 --保密加密

## 源码加密 编译行语言java

## 类库加密 使用自开发类库 非公开

## 数据加密（只有结合代码才能数据存储）

 数据安全 密码学原理与概论

1.1. 密码学方向（公钥方向） 2

1.2. 古典密码主要靠算法，现代靠密钥 2

1.3. 香农三大定理 2

2. 古典密码 3

2.1. 古典密码学可以分为代替密码（也叫做移位密码）和置换密码（也叫做换位密码）两种，其中代替密码典型的有Caesar密码，仿射变换等，置换密码有单表置换和多表置换等。 3

2.2. 维吉尼亚密码 3

3. 密码学原理与实践（第3版）》是密码学领域的经典著作 3

3.1. 第1章 古典密码学 3

3.2. 第2章 Shannon理论 香农理论 3

3.3. 第3章 分组密码与高级加密标准 3

3.4. 第4章 Hash函数 3

3.5. 第5章 RSA密码体制和整数因子分解 3

3.6. 第6章 公钥密码学和离散对数 3

3.7. 第7章 签名方案 3

3.8. 第8章 伪随机数的生成 3

3.9. 第9章 身份识别方案与实体认证 3

3.10. 第10章 密钥分配 4

3.11. 第11章 密钥协商方案 4

3.12. 第12章 公开密钥基础设施 4

3.13. 第13章 秘密共享方案 4

3.14. 第14章 组播安全和版权保护 4

4. 应用密码学：协议、算法与C源程序 4

5. 参考资料 4