北京郵電大學
Beijing University of Posts and Telecommunications

大数据安全
课程总结

石瑞生
网络空间安全学院

数据存储方

数据挖掘者

数据使用者

数据采集 → 数据存储 → 数据交易与流转 → 数据分析与挖掘 → 数据使用

大数据全生命周期安全管理

大数据采集	大数据存储	大数据流转	大数据处理
信息安全传输与匿名通信	大数据账号安全与访问控制	数据匿名化与差分隐私技术	大数据处理基础设施安全
在线追踪与隐私保护机制	数据完整性与隐私保护机制	保护隐私的可信计算	大数据处理算法的安全对抗

通用知识

- 大数据服务架构及其安全体系
- 密码算法
- 安全协议
- 攻防对抗
- 法律法规

CH1 绪论

CH2 基础知识

1）大数据安全相关的基本概念
2）密码学基础知识与安全概念（ GOAL-MODEL ）
5种**黑盒攻击模型**（COA，KPA，CPA，CCA，CCA2）； 2类安全目标（不可区分性，不可塑性）；4种常见的安全概念（ NM-CPA，NM-CCA，IND-CPA和IND-CCA ）

CH3 信息传输安全

CH4 身份管理与数据访问控制

1）TLS协议；证书安全（CT，钉扎），自动化证书；
2）身份认证：基本方法；FIDO协议
3）身份管理：2个SSO协议；认证Cookie

CH5 大数据存储与计算的安全隐私

CH6 保护隐私的可信计算

1）将数据存储在云端（数据加密机制），在云端计算（密文数据库），如何保证数据安全？
2）授权一个App使用你的数据做分析，又不想向App透漏你的数据，怎么办？
3）可信计算基：
应用系统，传统的访问控制与业务逻辑；CPU，SGX；密码算法，HE/MPC
可信基越小，安全性越高，但是计算成本高、速度慢；

CH7 数据匿名化与差分隐私

CH8 大数据算法安全与隐私

1）不使用原始的数据，也能够完成计算任务（例如，统计分析，模型训练等）
2）大数据算法，不仅仅是机器学习。

CH9 在线追踪与隐私保护

1）了解匿名通信技术的基本概念
2）了解在线追踪问题（以课本为主）