《数据安全》期末复习提纲

【成绩构成：平时点名等 5 分+实验报告 20 分+课程技术报告 15 分+试卷 60 分】

复习知识点：

1、数据生存周期：周期的概念，及不同阶段可能受到的数据安全威胁情况，以及应对方法、防护手段等；

2、安全属性（安全目标）：保密性、完整性、可用性，针对不同属性不同场景的可能攻击或破坏活动，以及可能的防护方法，DDoS 攻击，恶意代码，社会工程攻击等；

3、防火墙技术：防火墙功能，包过滤技术等；

4、入侵检测：IDS 功能，主机 IDS、网络 IDS，误报率，漏报率；

5、加密技术：公钥算法、私钥算法，典型的密码算法及其应用；

6、认证技术：数字签名、消息认证、身份认证等概念，以及作用；

7、数据库安全：拖库/洗库/撞库的概念以及目标能力，数据库加密方法，数据销毁；

8、 数据采集：最小够用原则，采集阶段的安全问题及保护方法；

9、 数据使用与处理：隐私数据，去标识化技术，重标识攻击，数据脱敏，常用去标识化技术及作用等；

10、大数据+AI 场景下，数据安全受到的新威胁，以及可能的保护方法.

题型示例：

选择题

1. 如果发送方使用的加密密钥和接收方使用的解密密钥不相同，从其中一个密钥难以推出另一个密钥，这样的加密系统称为（　　）。

   A）常规加密系统　　B）单密钥加密系统

   C）公钥加密系统　　D）对称加密系统

2. 能够在网络通信中寻找符合网络入侵模式的数据包而发现攻击特征的入侵检测方式是（　　）。

   A）基于网络的入侵检测方式　　B）基于文件的入侵检测方式

   C）基于主机的入侵检测方式　　D）基于系统的入侵检测方式

名词解释题

1. 最小够用采集原则
2. 数字签名

简答题、综合题

1. 为了保证两个用户端之间的网络通信安全性，需要进行数据加密和身份认证。请结合 RSA 等相关密钥算法，给出一种技术解决方案。（要求画出执行过程示意图和必要的解释）
2. 大数据智能场景下，可能遇到哪些新的数据安全问题？并简述可能的应对方法。