

北京邮电大学 2022——2023 学年第一学期

《大数据安全》期末考试试题（B 卷）

考试 注 意 事 项	一、学生参加考试须带学生证或学院证明，未带者不准进入考场。学生必须按照监考教师指定座位就坐。 二、书本、参考资料、书包等物品一律放到考场指定位置。 三、学生不得另行携带、使用稿纸，要遵守《北京邮电大学考场规则》，有考场违纪或作弊行为者，按相应规定严肃处理。 四、学生必须将答题内容做在试题答卷上，做在试题及草稿纸上一律无效										
考试 课程	大数据安全				考试时间			年 月 日			
题号	一	二	三	四	五	六	七	八	九	十	总分
满分											
得分											
阅卷 教师											

一、 填空题：（每空 1 分，共 20 分）

- 1.大数据技术在安全领域的应用，主要包括以下两个方面的内容：
_____和_____。
2. 发布-遗忘模型中数据匿名化的主要步骤：
_____, _____、_____和_____。
3. 容器技术的三个核心概念： _____、_____和_____。
- 4.访问控制技术是信息系统安全的核心技术之一，该技术中_____是请求访问的实体，_____是接受访问的实体，_____是主体对客体的访问规则集。
5. 在 Kerberos 协议中有两种票据，_____用于用户访问票据授权服务器，_____用于用户访问应用服务器。

6. 一次一密系统是否满足 NM(不可塑性, Non-malleability)的安全目标? _____。
7. 常见的容器安全问题有_____、_____、集群入侵。
8. 匿名属性包括_____和_不可联系性。
9. 安全多方计算模型中的参与者可以分为三类: _____、_____和恶意参与者。

二、 选择题: (每题 1 分, 共 10 分)

1. 发起者需要在发起匿名通信之前确定整个通信的传输路径的是 ()
- A. 基于 Mix 算法的匿名通信
 - B. 基于洋葱路由算法的匿名通信
 - C. 基于泛洪算法的匿名通信
 - D. Tor 匿名通信
2. 实现数据匿名化的主要方法有 ()
- A. 泛化
 - B. 抑制
 - C. 聚合
 - D. 过滤
3. 由于计算机的普及,很多攻击者具有更强大的计算能力。1979年,Robert Morris 和 Ken Thompson 提出了哈希加盐 (Hashing and Salting) 的方法来对口令进行加密处理,来抵抗字典攻击和暴力破解,并应用于 Unix 操作系统。以下哪些方法比哈希加盐的方法更安全? ()
- A. **PBKDF2**(Password-Based Key Derivation Function)
 - B. BCrypt

C. SCRYPT

D. Argon2

4. RSA 加密算法是（ ）

A. 对称密码算法

B. 公钥密码算法

C. 加法同态加密算法

D. 乘法同态加密算法

5. 遵循 K 匿名模型发布数据，数据集的披露风险小于（ ）

A. $1/K$

B. $2/K$

C. $1/(2 K)$

D. $1/(3 K)$

6. 以下哪些技术是用来解决仿冒证书问题的？（ ）

A. CT（certificate transparency）

B. HTTP Public Key Pinning（HPKP）

C. CDN

D. 自动证书管理环境(ACME)协议

7. 下述哪些陈述是正确的？（ ）

A. AES-CBC 加密方案是语义安全的

B. RSA 加密算法是语义安全的

C. AES-GCM 加密方案是语义安全的

D. ElGamal 加密算法是语义安全的

8. TLS 握手协议的任务包括：（ ）
- A. 协商密钥规格
 - B. 利用公钥证书来认证服务器的身份
 - C. 生成会话密钥
 - D. 用会话密钥加密传输的数据
9. 以下关于 FIDO 协议的论述哪些是正确的？（ ）
- A. FIDO 协议的在线身份认证协议采用了非对称公钥密码技术来提供安全保障
 - B. FIDO 协议包括本地身份识别与在线身份认证两部分
 - C. FIDO 协议支持指纹、语音、虹膜、脸部识别等生物身份识别方式
 - D. FIDO 协议的在线身份认证协议采用了对称密码技术来提供安全保障
10. 以下 HTTPS 的部署模式中，哪个是最安全的？（ ）
- A. HTTP 和 HTTPS 并存
 - B. HTTP 默认跳转到 HTTPS
 - C. 持久跳转 HTTPS(HSTS)
 - D. HSTS + HSTS Preload

三、 综合题（共 70 分）

1. QQ 浏览器（版本 6.5.0.2170）数据传输的安全问题分析

我们分析了 Android 浏览器版本 6.5.0.2170。

这个版本和更新后的 QQ Browser 服务器实现了以下步骤来加密从客户端到服务器端的 WUP 请求:

1. 首先，客户端为会话生成一个 128 位的 AES 会话密钥，使用伪随机数生成器 (PRNG)，其种子是自 Unix epoch 以来的以毫秒为单位的当前时间。
2. 然后，客户端使用 1024 位的 RSA 公钥对该会话密钥进行加密。公钥的指数是 65537，而 RSA 实现是“教科书式 RSA”（没有应用填充形式）。
3. 客户端使用 AES 会话密钥在 ECB 模式下加密 WUP 请求。
4. 客户端将 RSA 加密的 AES 会话密钥和加密的 WUP 请求发送给服务器。
5. 服务器使用自己的私钥对从客户端接收到的 RSA 加密的 AES 会话密钥进行解密，然后选择明文中最有效率的 128 位作为 AES 会话密钥。
6. 服务器使用通过 RSA 解密获得的 AES 会话密钥解密 WUP 请求。

如果从客户端接收到的 AES 密文正确地解密为有效的 WUP 请求，服务器将使用 AES 会话密钥发送一个 AES 加密的响应(也使用 ECB 模式)。

请分析以上数据传输模式的安全问题，并给出修复问题的方案。（10 分）

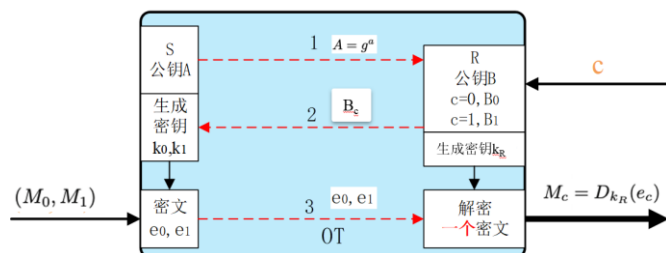
2. 隐私的定义、分类、及其度量与量化表示（10 分）

3. 阐述差分隐私的工作原理（10 分）

4. 数据可恢复性证明 POR 机制的基本思路（10 分）

5. 简述 K 匿名、L 多样性、T 相近隐私保护模型的基本思想及其存在的问题（10 分）

6. 参考下图，解释一下 1-out-of-2 OT 协议的工作原理。（10 分）



7. 同态加密（10 分）

- 1) 请给出同态加密的定义，
- 2) 证明：RSA 算法是乘法同态的；
- 3) 证明：Paillier 算法是加法同态的。

