北京邮电大学 2021——2022 学年第一学期

《大数据安全》期末考试试题（A 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											

装 订 线 封 线 密

专业：_____ 班级：_____ 学号：_____ 班内序号：_____ 姓名：_____

一、 填空题：（每空 1 分，共 20 分）

1.大数据安全包含_____和_____两重含义。

2. 匿名通信中，匿名属性包括不可辨识性和_____。

3. 安全多方计算模型可以分为_____和恶意模型。

4. 开放认证授权(OAuth)协议的四种模式：_____、_____、密码模式 和客户端模式。

5. 密码学的攻击模型可以分为黑盒模型、_____和_____。

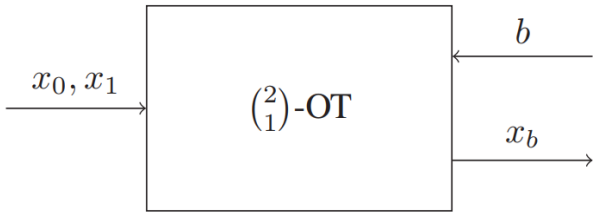
一个加密算法的明文和密文一样长，请问：该加密算法是语义安全的吗？___。

6. 差分隐私的通用随机算法有_____和指数机制。

7. TLS 协议可分为_____（负责密码组件的协商以及安全信道的建立）

和_____（在已建立的安全信道中传输秘密信息）。

8. 在下图的 2 选 1 不经意传输（OT）模型中，当 b=0 时，x_b=_____;



9. 容器技术的三个核心概念：镜像、_____和_____。

10. **在无限计算能力的攻击者模型下的安全的多方计算协议为_____的多方计算协议；**

在有限计算能力的攻击者模型下的安全的多方计算协议为_____的多方计算协议。

11. 发布-遗忘模型中数据匿名化的主要步骤包括：

识别身份信息、_____、_____和_____。

二、 选择题：（每题 1 分，共 10 分）

1. 下述哪些安全概念等价于语义安全（ ）

A. NM-CPA

B. IND-CCA

C. PRV$-CDA

D. IND-CPA

2. 下述哪些陈述是正确的？（ ）

A. AES 加密算法是语义安全的

B. RSA-OAEP 加密算法是语义安全的

C. AES-CTR 加密方案是语义安全的

D. 椭圆曲线加密算法是语义安全的

3. 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

4. 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采用了对称密码技术来提供安全保障

5. 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

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. 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

8. 容器与虚拟机相比较的优势有（ ）

A. 占用存储空间小，下载传输快

B. 消耗的 CPU 和内存更少

C. 启动速度更快

D. 更安全

9. Paillier 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

10. 静态数据发布原则 ***L*-diversity 保证发布数据集的披露风险小于（ ）**

A. ***1/L***

B. ***2/L***

C. ***1/(2L)***

D. ***1/(3L)***

三、 综合题 （共 70 分）

1. 隐私的定义、分类、及其度量与量化表示（10 分）

2. 阐述 SSL 握手协议的主要流程，然后分析一下 SSL 握手协议中 RSA 密钥交换的安全性，并提出改进方案。（10 分）

3. 解释一下姚氏混淆电路的工作原理。（10 分）

4. 某同学想用简单的示例验证一下 Paillier 同态加密算法，却惊讶地发现解密出来的明文不正确，不知道哪里出了错。

具体计算过程如下：

算法	示例: m=2
key generation： 1.随机选择两个大素数p和q； 2.计算n=pq，λ=lcm(p-1,q-1)，lcm是求两个数的最小公倍数。 3.随机选择基g，$g \in Z^*_{n^2}$，且满足 $\gcd(L(g^\lambda \bmod n^2), n) = 1$，其中L(x)=(x-1)/n 4.计算μ=（$L(g^\lambda \bmod n^2))^{-1} \pmod n$ 那么： 公钥pk=(n，g)； 私钥sk=(λ，μ)；	密钥生成： 1）取 p=3,q=5，计算得到 λ=lcm(2,4)=4 , n=15, 2）选取 g=11，计算出 u=1
Encryption: plaintext $m < n$ select a random $r < n$ ciphertext $c = g^m \cdot r^n \bmod n^2$ **Decryption:** ciphertext $c < n^2$ plaintext $m = \frac{L(c^\lambda \bmod n^2)}{L(g^\lambda \bmod n^2)} \bmod n$	1）加密： 取随机数 r=5，计算得到密文 c=50； 2）解密： 对 c 解密得到的明文 m’=11.6

请你指出该同学计算过程中哪里出现了错误，并给出一个正确的计算过程。（5 分）

5. 阐述加密数据去重的基本原理（10 分）

6. 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）

7. 安全多方计算问题（15 分）

1）请阐述姚期智提出的**百万富翁问题的解决方案，并对其正确性和安全性进行分析。**（9 分）

2）设计一个基于 OT 协议的百万富翁问题解决方案，并给出一个该 OT 协议的具体实现方案（如果能够给出课堂上没有讲过的 OT 协议实现方案，本题目可以获得额外加分）。（6 分）