**密码学第七次作业**

**1.【公钥密码体制基础知识】**

**（1）**相比于对称密码，公钥密码技术研究的基本工具不再是和，而是。

**（2）**公钥密码体制的组成部分：、、、、。

**（3）**公钥密码的应用：公钥密码体制除了和对称密码体制一样通过实现，还可以通过实现，此外还常用于。

**（4）**公钥密码实现保密和认证：若Alice使用公钥密码向Bob传输秘密信息，则应用的加密，用的解密；若Alice使用公钥密码向Bob提供签名，则应用的签名，用的验签。（本小题选填公钥/私钥，Alice/Bob）

**（5）**实际应用中多采用混合加密并提供认证服务：

I.通过生成种子；

II.输入种子，通过生成用于本次会话所需的随机数；

III.利用双钥体制通过或协商会话密钥；

IV.对消息进行，引入随机数来提供算法的非确定性；

V.将原消息与第IV步所得结果拼接进行，引入随机数来提供算法的非确定性。

A.对称加密 B.公钥加密 C.密钥交换 D.数字签名 E.TRNG F.PRNG

**（6）**请对比对称密码体制和公钥密码体制，从可满足的安全需求、算法吞吐量大小、密钥管理难度比较两者的优缺点。

**2.【RSA基础知识】**

**（1）**RSA算法描述：RSA体制基于的困难问题是，其密钥生成算法、加密算法、解密算法三元组可简记为。

I.密钥生成算法：

①通常通过安全参数构造或采用无参构造，选择至少位的大素数满足。

②计算和。

③选取指数，应满足。

④计算。

⑤导出公钥为，私钥为。

II.加密算法：

算法的输入（明文）满足，计算密文。

III.解密算法：

对于合法的密文，解密结果为。

**（2）**使用RSA进行加解密运算时，可以通过快速模幂算法加快指数运算的速度，也可以通过中国剩余定理加速解密。给定参数如下：，请使用计算器完成RSA的加解密，并使用快速模幂和中国剩余定理加速运算。

**3.【对Plain-RSA的攻击】**区别于引入不确定性的RSA-OAEP等构造方式，第2题给出的基础构造一般称为Plain-RSA（或“教科书式的RSA”），该方案具有较高安全隐患。请通过如下攻击方式攻破Plain-RSA：

**（1）**给定参数如下：，选取随机数如，请通过选择密文攻击得到消息。（已知：的解密结果是2504，的解密结果是2305）

**（2）**计算，与比较，该结果是巧合吗？请简述原因。

**4.**【Diffie-Hellman密钥交换】

**（1）**Diffie-Hellman密钥交换基于的数学问题是，它只能用于，不能用于或，基于同一困难数学问题构造的可实现上述功能的双钥密码体制是（写出一种即可）。

**（2）**给定参数如下：公共参数中素数。本原根，用户A的私钥，用户B的私钥，则用户A的公钥，用户B的公钥为，双方共享的密钥。

**（3）**该协议中每一方都选择一个秘密参数，给对方发送，其中公开。请说明，如果给对方发送的是，通信双方也能协商密钥，但敌手在不知道秘密参数的情况下可以攻破该系统。

**（4）**教材P217图10.2说明了针对Diffie-Hellman的中间人攻击可以生成两个不同的公私钥对。事实上，攻击者也可以更简单的只生成一组公私钥对完成中间人攻击，请简述这一过程。

**注意：**

以上作业请使用**pdf**文档格式提交，于**2023年4月23日（星期日）23:59**之前在OJ系统上提交，并将作业命名为“**学号\_姓名\_密码学第七次作业**”。如“21371234\_张三\_密码学第七次作业”。