**密码学第七次作业参考答案**

**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代换（代替）和置换，而是数学函数（陷门单向函数）。

**（2）**公钥密码体制的组成部分：明文、密文、公钥和私钥、加密算法、解密算法。

**（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加密实现保密性，还可以通过数字签名实现不可否认性（或身份鉴别、认证），此外还常用于密钥交换。

（本题填空有多种理解方式，对答案范围可以适当放宽）

**（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Bob的公钥加密，用Bob的私钥解密；若Alice使用公钥密码向Bob提供签名，则应用Alice的私钥签名，用Alice的公钥验签。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TRNG生成种子；

II.输入种子，通过PRNG生成用于本次会话所需的随机数；

III.利用双钥体制通过公钥加密或密钥交换协商会话密钥；

IV.对消息进行数字签名，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对称加密，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

EFBCDA（EFCBDA）

**（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。

对称密码体制：可满足保密性的要求，可构造数据完整性检验算法如哈希函数，消息真实性检验算法如MAC，但不能提供不可否认性；加解密速度快，运行效率高，密钥长度较短；密钥管理难度较大，往往每次会话都要重新生成密钥。

公钥密码体制：可满足数据保密性、数据完整性、认证性和不可否认性的要求；运算效率较低，其吞吐量往往比对称密码算法低2~3个数量级；借助于公钥基础设施，可以实现有效的密钥管理，更适应多用户间两两通信的互联网时代特点。

**2.【RSA基础知识】**

**（1）**RSA算法描述：RSA体制基于的困难问题是大整数分解，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1024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。

密钥生成：计算。

加密：。（需要快速模幂，略）

不使用CRT的解密：。（需要快速模幂，略）

使用CRT的解密：

**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。

原因：不是巧合，任取明文消息都成立。

由拓展的欧拉定理：，

有，

计算可知

因为，

所以。

若，

易知或，

可用基本的欧拉定理求解，略。

（本题合理即可）

**4.【Diffie-Hellman密钥交换】**

**（1）**Diffie-Hellman密钥交换基于的数学问题是求解离散对数的困难性，它只能用于密钥交换，不能用于加解密或数字签名，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Elgamal密码体制（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。

正确性：设另一方的秘密参数为，给对方发送，双方协商的密钥是。

安全性：因为和公开，因此敌手直接把两个值模乘获得协商的密钥，该方案不安全。

**（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。

攻击者D生成；

攻击者D用替换A发给B的；

B计算得到密钥；

攻击者D用替换B发给A的；

A计算得到密钥；

攻击者可同时计算和。