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_加密算法_和_密钥_____，而是____数学算法和数字证书____。

（**2**）公钥密码体制的组成部分：__明文__、_密文__、__公钥__、__私钥___、__加密算法_。

（**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__加密解密__实现__机密性保护_，还可以通过_数字签名_实现__认证和完整性保护_，此外还常用于__密钥协商_。

（**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___E___生成种子；

II.输入种子，通过___F___生成用于本次会话所需的随机数；

III.利用双钥体制通过___A___或___C___协商会话密钥；

IV.对消息进行___B___，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___D___，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。

可满足的安全需求：

对称密码体制的安全性主要基于密钥长度和算法的强度，攻击者需要猜测密钥才能破解密码。公钥密码体制的安全性则依赖于数学难题，例如大整数分解和离散对数问题等，攻击者需要解决这些难题才能破解密码。因此，公钥密码体制安全性更强。

算法吞吐量大小：

对称密码体制的加密和解密算法通常比公钥密码体制的算法快得多，因为对称密码体制的算法使用的密钥长度比公钥密码体制的密钥短得多，并且在算法上公钥密码体制经常用到大整数的模幂运算，速度较慢，而对称密码的扩散和混淆对计算资源的需求更下。对称密码体制的加密和解密速度通常比公钥密码体制快得多，因此对称密码体制更适合在大数据传输等高吞吐量场景下使用。

密钥管理难度：

对称密码体制的密钥管理更加困难，因为在通信双方之间共享同一个密钥，如果密钥泄露，攻击者可以轻松地解密通信内容。对密钥分发和变更过程中的很难有安全保障。公钥密码体制的密钥管理更加

容易，因为每个通信方都有自己的密钥对，而且公钥可以自由传播，私钥只需要在本地保存即可。

2.【RSA 基础知识】

（1）RSA 算法描述：RSA 体制基于的困难问题是__大整数分解问题__，其密钥生成算法、加密算法、解密算法三元组可简记为(Gen, Enc, Dec)。

I.密钥生成算法 Gen：

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 p,q 满足 $p \neq q$。

②计算___n___和__Φ（n）__。

③选取指数 e，e 应满足_（e,Φ(n)) = 1)___，__e 不能太小__。

④计算__d____。

⑤导出公钥为___d___，私钥为__e____。

II.加密算法 Enc：

算法的输入（明文 M）满足 $M < n$，计算密文 $C =$ _M^e(mod n)_。

III.解密算法 Dec：

对于合法的密文 C，解密结果为 $M =$ __C^d(mod n)__。

（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：$p = 37$,$q = 73$,$e = 17$,$M = 2039$，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。

不使用快速模幂：

1. n = p*q = 2701， Φ(n) = 2592，
2. e*d = 1 mod 2592 ➞ d = 305
3. e = 0b10001
4. 快速模幂得：C = 1878
5. 解密：分成两个方程：M = C^d mod p , M = C^d mod q
6. C^d mod p 快速模幂解得 4，C^d mod q 解得 68
7. 根据中国剩余定理，a1 = 4， a2 = 68，m1 = 37 , m2 = 73 , m = 2701
8. t1 = 36 , t2 = 2
9. M = a1*m1*t1+a2*m2*t2 mod n = 2039

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：$n = 2701, e = 17, C = 1878$，选取随机数如 $r = 123$，请通过选择密文攻击得到消息 M。（已知：rC 的解密结果是 2504，r^eC 的解密结果是 2305）

$(rC)^d = M_1 \bmod n$，$(r^eC)^d = rC^d = M_2 \bmod n$，$\rightarrow C^d = M_2 r^{-1} \bmod n$，
$(C^d)^{-1} = M_2^{-1} r^1$，$(rC)^d (C^d)^{-1} = r^d = M_1 M_2^{-1} r = 1514 \bmod n$，我们发现，
$r^e = 1514 \bmod n$ 根据有限域的知识，得到$d = e = 17$

$$M = C^d \bmod n = 1323$$

（2）计算$M^{'} = C^e \, mod \, n$，与 M 比较，该结果是巧合吗？请简述原

因。

$M' = C^e \bmod n = 1323 = M$，这是因为$e$和$d$本身就相等啊

4.【Diffie-Hellman 密钥交换】

（**1**）Diffie-Hellman 密钥交换基于的数学问题是_离散对数问题__，它只能用于__密钥交换__，不能用于__加密___或__认证_____，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_RSA 加密算法___（写出一种即可）。

（**2**）给定参数如下：公共参数中素数 $q = 71$。本原根$\alpha = 7$，用户 A 的私钥$X_A = 5$，用户 B 的私钥$X_B = 12$，则用户 A 的公钥$Y_A =$ __51_____，用户 B 的公钥为$Y_B =$ __4_____，双方共享的密钥 $K =$ ___58___。

（**3**）该协议中每一方都选择一个秘密参数 x，给对方发送$\alpha^x \, mod \, q$，其中α公开。请说明，如果给对方发送的是$x^\alpha \, mod \, q$，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。

A的公钥$Y_A = x^\alpha \bmod q$，B的公钥$Y_B = y^\alpha \bmod q$，B拿到A的的公钥后，$K = Y_A Y_B \bmod q$，A拿到B的公钥后计算。形$K = Y_A Y_B \bmod q$成一个共享密钥，达到协商密钥的效果。

但是$Y_A Y_B$　q都是公开的，攻击者很容易破解$K = Y_A Y_B \bmod q$

（**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。

Alice发送公钥$Y_A = \alpha^{X_A} \bmod q$，中间攻击则得到这个值，进行加工$Y_{AD} = Y_A^{X_D} \bmod q$，发送给Bob，Bob收到后，计算共享秘密密钥$K = Y_{AD}^{X_B} = \alpha^{X_A X_B X_D} \bmod q$，再将公钥$Y_B = \alpha^{X_B} \bmod q$发送给中间攻击者，在计算$Y_{BD} = Y_B^{X_D} \bmod q$，再发往Alice，Alice计算共享公共密钥$K = Y_{BD}^{X_A} \bmod q$。

对于中间攻击者，已知Y_{AD}和Y_{BD}，根据$\alpha^{-X_D} \bmod q$，攻击者可以算得$K = Y_{AD}Y_{BD}\alpha^{-X_D} \bmod q$，达到破解的功能

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”。