RSA 密码破译

一． 问题描述

RSA 密码算法是使用最为广泛的公钥密码体制。该体制简单且易于实现，只需要选择 5 个参数即可（两个素数p和q、模数$N = pq$、加密指数e和解密指数d）。设m为待加密消息，RSA 体制破译相当于已知$m^e \ mod \ N$，能否还原m的数论问题。目前模数规模为 1024 比特的RSA 算法一般情况下是安全的，但是如果参数选取不当，同样存在被破译的可能。

有人制作了一个 RSA 加解密软件（采用的 RSA 体制的参数特点描述见密码背景部分）。Alice 使用该软件发送了一个通关密语，且所有加密数据已经被截获，请问能否仅从加密数据恢复该通关密语及 RSA 体制参数?

在示例中，提供了这个软件发送某个明文的所有参数和加密过程的全部数据。

二． 密码背景

RSA 密码算法描述如下，包含体制参数选取和加解密过程。

1）RSA 体制参数选取

Step1. 每个使用者，任意选择两个大素数p和q，并求出其乘积$N = pq$。

Step2. 令$\varphi(N) = (p-1)(q-1)$，选择整数e，使得$GCD\big(e, \varphi(N)\big) = 1$，并求出$e$模$\varphi(N)$的逆元$d$，即$ed \equiv 1 \ mod \ \varphi(N)$.

Step3. 将数对(e, N)公布为公钥，d保存为私钥。

2）加解密过程

Bob 欲传递明文m给 Alice，则 Bob 首先由公开途径找出 Alice 的公钥(e,N)，Bob 计算加密的信息c为：$c \equiv m^e \ mod \ N$。

Bob 将密文c传送给 Alice。随后 Alice 利用自己的私钥d解密：

$$c^e \equiv m^{ed} \equiv m \ mod \ N$$

Alice 使用的 RSA 密码体制，有以下事项需要说明：

1） 模数$N = pq$规模为 1024 比特，其中p，q为素数；

2） 素数p由某一随机数发生器生成；

3） 素数q可以随机选择，也可以由 2）中的随机数发生器产生；

4） 可以对文本加密，每次加密最多 8 个明文字符；

5） 明文超过 8 个字符时，对明文分片，每个分片不超过 8 个字符；

6） 分片明文填充为 512 比特消息后再进行加密，填充规则为高位添加 64 比特标志位，随后加上 32 比特通信序号，再添加若干个 0，最后 64 比特为明文分片字符对应的 ASCII 码（注：填充方式参见加密案例，但注意每次通信的标志位可能变化）；分片加密后发送一个加密帧数据，帧数据文件名称为 dataX， 其中 X 表示接收序号，该序号不一定等于通信序号；

7） 帧数据的数据格式如下，其中数据都是 16 进制表示，结构如下

1024bit 模数N ｜ 1024bit 加密指数e ｜ 1024bit 密文$m^e \ mod \ N$。

8） 由于 Alice 初次使用该软件，可能会重复发送某一明文分片。

三． 提示（重要！！！）

你可以尝试从以下方向对密码进行破解：

1. 直接对N进行分解：pollard-rho和pollard's p-1算法等

2. 当e比较小的时候，可以对e进行攻击：低加密指数攻击等

四． 要求

1. 至多2人一组，没有额外计算力的支持。

2. 对RSA加密系统进行比较深入的了解，明白如何选取合适的N使得RSA系统更难被破解。

3. 尝试对这20个密码进行破解。解密代码必须在较短时间内完成对密码的破解。

五． 评分标准

1. 提交报告和对应的解密代码。

2. 最终不会以破解的数量作为优劣的判断标准（希望通过这个project，大家对于密码学有更多的了解）。（当然，如果你一个也没有破解出来，请及时向大家寻求帮助）