第三届（2018）全国高校密码数学挑战赛

赛题三

一、赛题名称：离散对数求解问题（Discrete Logarithm Problem）

二、赛题描述：

2.1 问题描述

设p是一个素数，g是模p剩余类群中的非零元素。已知模数p，g和y，求解x满足同余方程$y \equiv g^x (mod\ p)$的计算数论问题，称为模p剩余类域中离散对数求解问题。DH（Diffie-Hellman）密钥交换协议是 20 世纪 70 年代由 Whitfield Diffie 和 Martin Hellman 共同提出的，在网络安全中有着广泛的应用，其目的是让参与两方能够共享一个秘密信息（密钥）。DH 密钥交换协议的过程如下图：

A 发起方	B 应答方
产生 x_a并计算$y_a \equiv g^{x_a} mod\ p$	产生x_b并计算$y_b \equiv g^{x_b} mod\ p$
A 使用公共信道把 y_a发送给 B	B 使用公共信道把y_b发送给 A
接收到y_b并计算${y_b}^{x_a} (mod\ p)$	接收到y_a并计算${y_a}^{x_b} (mod\ p)$
此时，A 有信息 ${y_b}^{x_a} \equiv g^{x_b x_a}\ (mod\ p)$，B 有信息${y_a}^{x_b} \equiv g^{x_a x_b}\ (mod\ p)$，而 $g^{x_a x_b} \equiv g^{x_b x_a}\ (mod\ p)$。 这样，A 和 B 就得到了共同的信息。	

DH 协议的安全性基于素域（模素数p剩余类域）上离散对数求解的困难性。如果第三方可以在公共信道截获y_a和y_b，通过求取离散对数x_a，就可求出 A 和 B 的共同信息

$$ {y_b}^{x_a} \equiv g^{x_b x_a}\ (mod\ p) $$

本赛题要求利用合适的算法求解附件中给定参数的模p剩余类域中离散对数挑战问题，并获取 DH 密钥交换协议中的共同信息。随同赛题，我们给出了（但不限于）两个常用的软件包供选手参考使用。

2.2 赛题要求和评分标准

1）了解求解离散对数问题的基本原理和通用方法，熟悉常见离散对数计算软件包的使用（特别是附件中给出的 cado-nfs，NTL（数论库）等）；

2）尝试求解附件文件中的 DH 离散对数问题，给出结果，并简述求解原理、步骤和实现效率（包括使用的计算平台的基本性能，计算需要的时间和空间等）；

3）对无法完成求解的问题，试分析原因，根据数域筛法的基本原理，分析算法流程，优化各步参数，给出实现方案并评估计算量，尝试提出更好的解决方案。

三、密码学背景及相关研究进展

求解离散对数问题常见的算法有：Shanks 的大步小步算法(baby-step giant step algorithm)、Pollard rho 算法、Pohlig-Hellman 算法、Index Calculus 算法等。对于十进制三十位以上的素数，已知最优的模p剩余类域中离散对数求解算法是应用了数域筛法技术的 Index Calculus 算法。以下是国际上对该问题的一些求解纪录：

On 18 June 2005, Antoine Joux and Reynald Lercier announced the computation of a discrete logarithm modulo a 130-digit (431-bit) strong prime in three weeks, using a 1.15 GHz 16-processor HP AlphaServer GS1280 computer and a number field sieve algorithm.

On 5 February 2007 this was superseded by the announcement by Thorsten Kleinjung of the computation of a discrete logarithm modulo a 160-digit (530-bit) safe prime, again using the number field sieve. Most of the computation was done using idle time on various PCs and on a parallel computing cluster.

On 11 June 2014, Cyril Bouvier, Pierrick Gaudry, Laurent Imbert, Hamza Jeljeli and Emmanuel Thomé announced the computation of a discrete logarithm modulo a 180 digit (596-bit) safe prime using the number field sieve algorithm.

On 16 Jun 2016 08:27:11，Thorsten Kleinjung announced a new record computation of discrete logarithms modulo a 768 bit prime using the number field sieve.

四、参考文献

1. D. Coppersmith, A. Odlyzko, and R. Schroppel, *Discrete logarithms in* F*p*, Algorithmica

1(1986), 1–15. MR **87g:**11167.

2. D. Weber, *Computing discrete logarithms with the number field sieve*, Proceedings of the ANTS-II conference, Lecture Notes in Computer Science, vol. 1122, Springer–Verlag, 1996. MR **98k:**11186
3. Antoine Joux And Reynald Lercier, Improvements To The General Number Field Sieve For Discrete Logarithms In Prime Fields.A Comparison With The Gaussian Integer Method. Mathematics Of Computation Volume *72, Number 242, Pages 953–967 S 0025-5718(02)01482-5 Article electronically published on November 4, 2002.*
4. W Diffie and M Hellman, “New Directions in Cryptography”, IEEE Trans. Information Theory 22 (1976) pp 472–492.
5. D Gordon, “Discrete Logarithms in GF(p) using the Number Field Sieve”, SIAM J. Disc. Math. 6(1) (1993) pp 124–138.
6. 《公开密钥密码算法及其快速实现》周玉洁，冯登国编著，国防工业出版社，ＩＳＢＮ７－１１８－０２７４９－９／ＴＰ．６９０。