Homework 2

2017年3月8日 18:28

HW2. Large number arithmetic

Description

- Write a +-*/ algorithm for large integers. (10 point)
- Implement the DH algorithm. (5 point)

Deliverables

Mail the deliverables to TA, with title: SEC2017-HW2-ID-NAME

- The source code
- The executable (win / linux / mac)

Deadline

- 23:59:59, Apr. 2th, 2017

https://tools.ietf.org/html/rfc7296#page-137
https://www.ietf.org/rfc/rfc3526.txt

B.1. Group 1 - 768-bit MODP
This group is assigned ID 1 (one).
The prime is: 2^768 - 2 ^704 - 1 + 2^64 * { [2^638 pi] + 149686 }
Its hexadecimal value is:
FFFFFFFF FFFFFFFF C90FDAA2 2168C234 C4C6628B 80DC1CD1
29024E08 8A67CC74 020BBEA6 3B139B22 514A0879 8E3404DD
EF9519B3 CD3A431B 302B0A6D F25F1437 4FE1356D 6D51C245
E485B576 625E7EC6 F44C42E9 A63A3620 FFFFFFFF FFFFFFFF
The generator is 2.
B.2. Group 2 - 1024-bit MODP
This group is assigned ID 2 (two).
The prime is 2^1024 - 2^960 - 1 + 2^64 * { [2^894 pi] + 129093 }.
Its hexadecimal value is:
FFFFFFFF FFFFFFFF C90FDAA2 2168C234 C4C6628B 80DC1CD1
29024E08 8A67CC74 020BBEA6 3B139B22 514A0879 8E3404DD
EF9519B3 CD3A431B 302B0A6D F25F1437 4FE1356D 6D51C245
E485B576 625E7EC6 F44C42E9 A637ED6B 0BFF5CB6 F406B7ED
EE386BFB 5A899FA5 AE9F2411 7C4B1FE6 49286651 ECE65381
FFFFFFFF FFFFFFFF
The generator is 2.

http://blog.csdn.net/u014298090/article/details/22116769