大数据安全大作业
Shamir秘密共享

1 秘密共享

有时候，秘密不能由一个人独自掌握，而需要多人参与才能打开秘密，比如说核导弹发射密码，我们不想让一个人独自握有发射密码以防泄露等特殊情况，为此我们需要把密码分给多人，每个人握有用于恢复密码的部分信息，握有子秘钥的一定人数的人可以恢复密码发射核弹。这种技术被称为秘密分割(secret splitting)或秘密分享(secret sharing)。
假设存在一个秘密s，现在需要把秘密分给n个用户$P_1, ..., P_n$，每个人获得一部分信息s_i，这部分信息被称为一个子秘钥或影子(share or shadow)，需要至少t个用户提供他们所拥有的子秘钥才能恢复出秘密s，这样一种方案被称为(t,n)门限秘密共享方案。如果任意t-1个用户提供他们的子秘钥都无法获得关于s的任何信息，就称该方案是完善的。

2 Shamir秘密共享

Setup:首先构建一个有限域GF(q)上的多项式f(x)=$a_0 + a_1x + ... + a_{t-1}x^{t-1}$，其中q为素数，秘密为$a_0$即f(0)，$a_0 < q$。
秘密分割:然后在f(x)上均匀随机选取n个不同的点$(x_1, y_1), ..., (x_n, y_n)$并分发给n个人，$n < q$。
秘密恢复:通过任意t个点可以恢复出秘密a_0，可以通过代入t个点的坐标然后解t元一次方程组来算出a_0。但也可以通过拉格朗日插值法更快的得出a_0，具体公式如下：

$$a_0 = f(0) = \sum_{j=0}^{t-1} y_j \prod_{\substack{m=0 \\ m \neq j}}^{t-1} \frac{x_m}{x_m - x_j}$$

3 作业要求

使用**C++**或**python**语言，实现Shamir秘密共享算法。要求实现两个函数*SecretDistribution*和*SecretRecovery*，函数描述由以下伪代码给出，main函数将用于测试实现的两个函数，main函数请一并提交。
使用C++请提交相应的.h和.cpp文件，使用python请提交相应的.py文件。
注意：请保持函数名的一致性。
建议q选得稍大些，可以额外写一个素数生成函数。
截止日期：2021/7/4

4 Reference

[1] Shamir, Adi. "How To Share A Secret". Communications Of The ACM, vol 22, no. 11, 1979, pp. 612-613. Association For Computing Machinery (ACM), doi:10.1145/359168.359176.

Algorithm 1 Shamir Secret Sharing

function main()
$filename$ ←a string
$n, t, s \leftarrow$ some integers
SecretDistribution(n,t,s,filename)
r ←SecretRecovery(filename)
if r==s **then**
    success
else
    fail
end if
end function

function SecretDistribution(n, t, s, filename)
Input: total number of shares n, threshold t, secret s, name of file for storage $filename$.
Output: 0 or -1 in case of exception.
Description: This function picks prime number q, constructs f(x) and generates n shares. Then it writes f(x),q, t and n shares (x_i, y_i) into a file called "$filename$" in the current folder.
end function

function SecretRecovery(filename)
Input: name of file for storage $filename$.
Output: secret r or -1 in case of exception.
Description: This function reads from a file called "filename". Then it shows n,t and asks user to input t numbers between 1 and n. Then it shows the corresponding shares and tries to recover the secret using the shares.
end function