密碼學期末專題完成狀況

參考資料 https://latticehacks.cr.yp.to/ntru.html

目前已完成部分:

mod(a, n): 取模後回傳的值落在n/2到-n/2之間

modinv(a, m): a為純量，回傳a在Zm中的乘法反元素

balanced\_mod(f, p): f為向量，p為純量，f的所有係數皆模p，且係數落在p/2到-p/2之間

多項式運算(多項式皆以numpy array表示，依array index小到大降冪排列)

poly\_add(x, y): 多項式加法

poly\_minus(x, y): 多項式減法

poly\_scalar(a, x): a為純量，多項式純量乘法

poly\_mul(x, y): 多項式向量乘法

random\_d\_poly(d, n): 產生一隨機多項式(加密的過程中使用)，其中包含d個非零的數(1和-1)，以及n-d個零

convolution(f, g, n): 實現多項式模XN-1的過程

poly\_div(x, y, p): 多項式在係數模p下的除法

未完成部分:

ext\_eculid(x, y, p, n): 回傳模反多項式