Schnorr：

屬於**交互式零知識證明**，以**離散對數之難度**作為核心，***Prover*** 知道一個秘密私鑰 x，計算 $y \equiv g^x (mod\ p)$，並提供 ***Verifier*** 公鑰 (p, g, y)，***Prover*** 欲在不透漏 x 的情況下，讓 ***Verifier*** 相信其知道秘密 x ，以下為參數設定：

質數：p：隨機挑選的大質數

q： $q \mid (p-1)$

生成元（$generator$）：$g \in F_p^*$

私鑰：x （**隨機挑選**）

公鑰：(p, q, g, y)

1. **承諾（commit）：**
   (1) ***Prover*** 隨機選擇一個 ephemeral key s ，使得 $s \in \{1 \ldots . (q-1)\}$。
   (2) 計算承諾值 f： $\boxed{f = g^s\ (mod\ p)}$。
   (3) 傳送 f 給 ***verifier***。
2. **挑戰（Challenge）：**
   (1) ***Verifier*** 產生一個隨機的挑戰值 c ，使得 $c \in \{1 \ldots . (q-1)\}$。
   (2) 傳送 c 給 ***Prover***。
3. **回應（Response）：**
   (1) ***Prover*** 計算： $\boxed{r = s + c\ x\ (\text{mod}\ q)}$ 。
   (2) 傳送 r 給 ***Verifier***。
4. **回應（Response）：**
   (1) ***Verifier*** 驗證： $\boxed{g^r \equiv f \cdot y^c (\text{mod}\ p)\ ?}$
   （成立 → 接受；不成立 → 拒絕）
   (2) $g^r = g^{s+cx} = g^s \cdot g^{cx} = f \cdot g^{cx} = f \cdot (g^x)^c = f \cdot y^c$

給 Chatgpt 的設計需求：

基於我的演算法實作，有以下要求：

1. 以 python 為程式語言，給我程式碼。
2. 演算法提到的參數要一致。
3. 執行 100 回合
4. 每一回合重點地方都要秀出 log，最後要有統計結果，並將結果匯出成 result.txt (輸出於當前位置)
5. 程式碼開頭：
   #ZKP with Schnorr
   #Author: 林伯叡、黃杭霆
   # Date: 2025/05/08
6. 函式上方要有中文註解，包含：函式名稱、輸入參數、回傳值、函數功能…等。