Protocole ? :
(personne qui offre, personne qui reçoit) La partie soulignée est celle que l'on souhaite chiffrer. Le système connaîtra les couples, les participants non.

1er protocole

Soit n participants
On associe chaque participants à un nombre : 1, 2, 3 …, n
On prend p, q premiers (Si on veut que chaque participant puisse avoir une clé privé distincte des autres, il faudra prendre q >= n. Non nécessaire cependant dans cet usage d'assurer l'unicité des clés)

On associe à chaque participant une clé privé X (on admet qu'il l'a connait, étant un secret santa on peut imaginer plein de manière de lui transmettre) (*)
On note PX la clé publique associé à la clé X

Notre programme détermine les couples (secretsanta_basique)
Avant de renvoyer, on chiffre le deuxième élément du couple avec la clé publique associé au premier élément du couple
On renvoie le couple chiffré, que seul le bon participant pourra déchiffrer en étant sûr de tomber sur son binôme (Deux personnes peuvent avoir la même clé, pas dérangeant car "l'imposteur" ne pourra pas le savoir. En déchiffrant le couple d'un autre, on obtiendra forcément un nombre mais on aucune manière de savoir si il s'agit du bon nombre ou non)

2e protocole

On ajoute une étape de transfert de clé à (*)

Difficultés de programmation : comment trouver g pour un p et q quelconque de manière efficace ? (On peut juste tester pour tout i jusqu'à en trouver un qui marche mais peut être coûteux en temps ? Négligeable face à la vitesse de calcul ?)