Algorithme de génération d'une adresse CGA
(source : livre de Gisèle Cizeault)

Ceci suppose qu'on possède une paire de clés publique/privée.

La génération d'une adresse CGA devrait s'effectuer ainsi:

Affecter au **Modifieur** une valeur pseudo-aléatoire sur 128 bits
Concaténer de gauche à droite le **Modifieur**, 9 octets de valeur 0, la clé publique encodée (format DER), et les éventuels champs d'extension. Appliquer l'algorithme SHA-1 sur cette concaténation. Prendre les 112 bits les plus à gauche de la valeur SHA-1. Le résultat est **Hash2**
Comparer les 16***Sec** bits les plus à gauche de **Hash2** avec 0. S'ils sont tous nuls, alors continuer à l'étape 4. Sinon, incrémenter le **Modifieur** de 1 et revenir à l'étape 2.
Affecter 0 au champ **Collision**.
Concaténer de gauche à droite la valeur finale du **Modifieur**, le préfixe réseau, le compteur de collision, la clé publique encodée, et les éventuels champs d'extension. Appliquer l'algorithme SHA-1 sur cette concaténation. Prendre les 64 bits les plus à gauche de la valeur SHA-1. Le résultat est **Hash1**
Fabriquer un identifiant d'interface à partir de **Hash1** en insérant la valeur de Sec dans les 3 bits les plus à gauche, et en mettant à zero les bits u et g.
Concaténer les 64 bits du préfixe réseau aux 64 bits de l'identifiant d'interface de façon à former une adresse IPv6 standard : avec ma partie préfixe à gauche et la partie interface sur la droite.
Effectuer une détection de collision d'adresses (DAD). En cas de collision, incrémenter le compteur de collision et aller à l'étape 5. Après 3 collisions, l'algorithme s'arrête et rapporte une erreur.
Former la structure des paramètres CGA en concaténant de gauche à droite : le Modifieur final, le préfixe réseau, le compteur de collision final, la clé publique encodée, et d'éventuel champs optionnels.

NB : **Sec** est entre 0 et 7.

En sortie, cet algorithme de génération produit une nouvelle adresse CGA et une nouvelle structure de paramètres CGA.