Le druide Gépégix et ses secrets
(une métaphore du chiffrement)

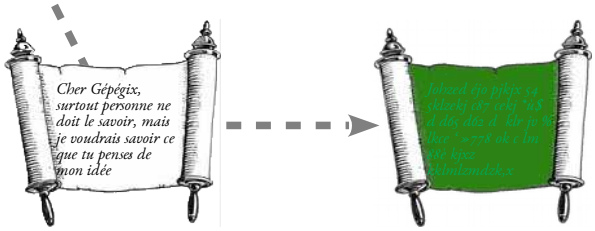
Le druide Gépégix reçoit des lettres du monde entier de personnes souhaitant profiter de ses talents de divination.

Par exemple un chef de clan souhaite savoir si c'est le bon moment pour attaquer son ennemi ou un garçon veut savoir si sa jolie voisine est amoureuse de lui.

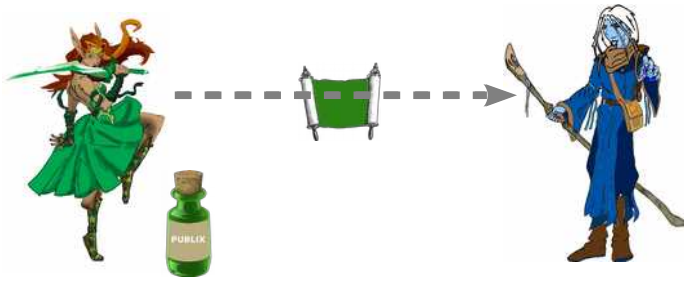
Le problème du druide est qu'il veut bien répondre à ces questions, mais il ne souhaite pas que tous ces secrets tombent entre de mauvaises mains.

Il a alors une idée, il s'enferme dans son laboratoire et il invente deux potions.

La première, Publix, est une potion toute verte. Quand on la verse sur un parchemin, les lettres se brouillent, tout devient vert et on ne peut plus lire ce qu'il y a d'écrit.



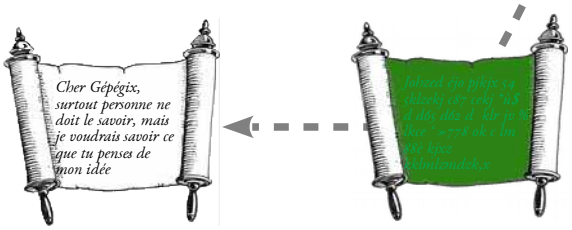
Le druide produit en grande quantité cette potion, qu'il distribue dans le monde entier.



À présent quand quelqu'un veut lui envoyer une requête, il verse du Publix dessus et la requête devient illisible.

La seconde potion que le druide a inventée, Privix, est une potion toute rouge.

Quand on la verse sur un parchemin couvert de Publix, elle annule le brouillage causé par le Publix et le texte redevient lisible.



Gépégix garde bien caché ses réserves de Privix, car c'est la seule potion qui permet de déchiffrer le Publix et lui seul en connaît la formule.

Ainsi, grâce aux potions Publix et Privix, les secrets transmis à Gépégix sont bien gardés.

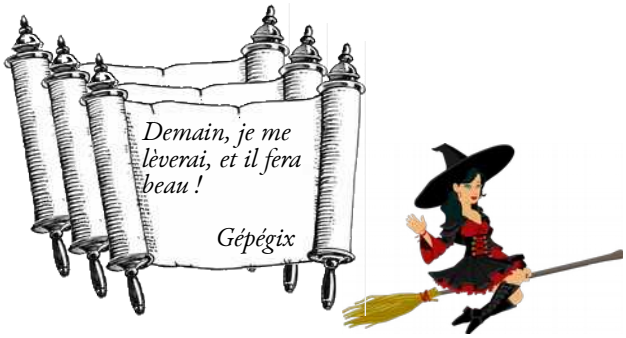
picasoft

Attribution - Pas d'Utilisation Commerciale - Partage dans les Mêmes Conditions 3.0 France
(CC BY-NC-SA 3.0 FR)

http://picasoft.net

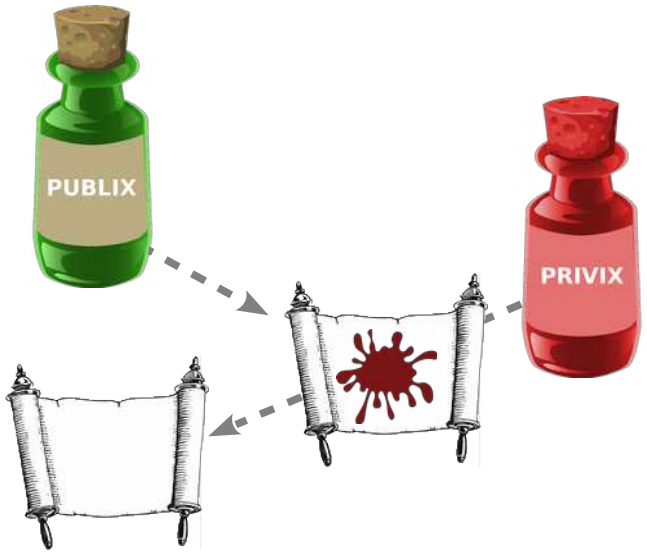
Les prophéties authentiques de Gépégix
(une métaphore de la signature)

Le druide Gépégix est reconnu dans le monde entier pour la qualité de ses prophéties. Il les inscrit sur des parchemins qu'il livre à des messagers qui vont les distribuer dans le monde entier.

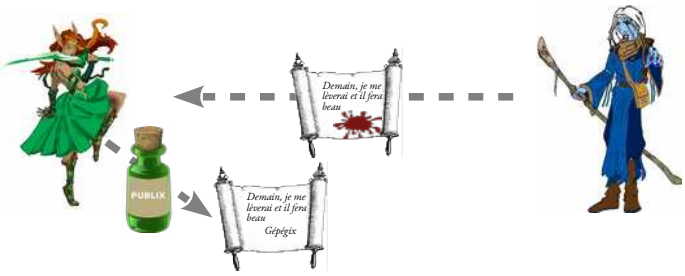


Malheureusement il existe des devins moins habiles que lui qui usurpent son identité pour faire passer de fausses divinations pour les siennes.

Gépégix a trouvé une parade en découvrant que l'on pouvait utiliser le Publix et le Privix dans les deux sens. Quand on verse du Publix vert du Privix rouge, cela le fait disparaître.



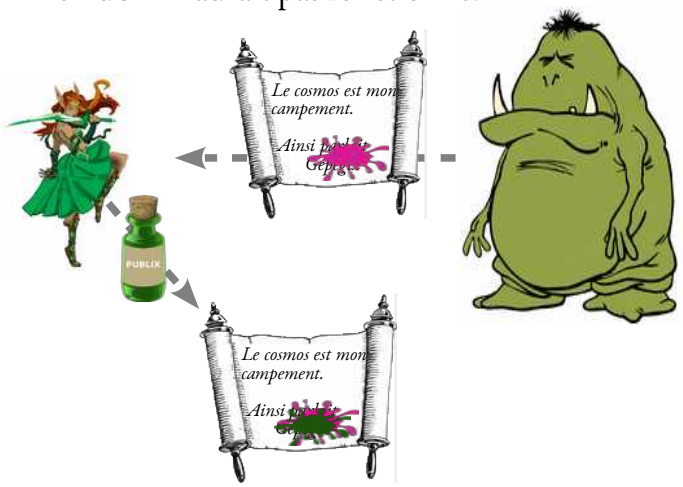
Ainsi il prend soin de signer chacune de ses prophéties en versant quelques gouttes de Privix dessus.



Quand quelqu'un reçoit un parchemin, il verse un peu de Publix dessus, si le rouge disparaît cela prouve que c'est bien un des messages de Gépégix.

En effet seul Gépégix dispose du Privix, et le Publix ne fonctionne que sur le Privix.

Donc si un imposteur avait signé avec une potion à lui, par exemple de l'Impostix, alors le Publix n'aurait pas fonctionné.



picasoft

Réalisé avec des images libres

CC BY NC SA

http://picasoft.net

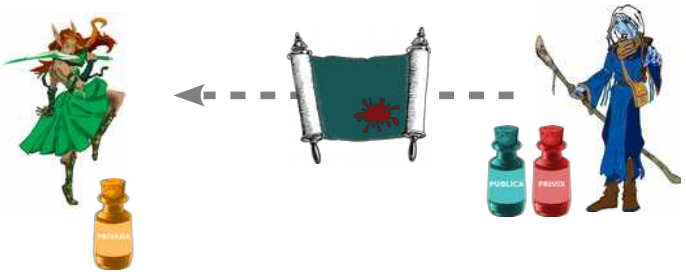
Gépégix et le conseil des druides
(une métaphore du chiffrement et de la signature de mails)

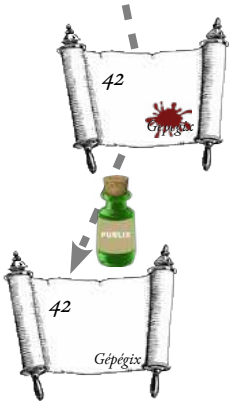
Fort de ses expériences, Gépégix propose un système de communication au conseil des druides, qui permettra à la fois de communiquer sans que personne ne puisse lire les messages interceptés, et en même temps de s'assurer de qui est l'expéditeur de chaque message.

D'abord il explique à chaque druide comment produire ses propres potions, afin qu'elles aient les mêmes propriétés que Publix et Privix, mais que chaque couple de potion soit unique.

Par exemple sa collègue Pégépa a réussi a créer une potion turquoise Publica ainsi qu'une orange Privada qui fonctionnent toutes les deux comme Publix et Privix, mais dont seul Pégépa connaît la formule.

Quand Gépégix envoie un message à Pégépa, il verse du Publica turquoise sur son message et signe avec quelques gouttes de Privix rouge.





Quand Pégépa reçoit le message, elle verse du Privada orange sur le message pour pouvoir le lire, et du Publix vert sur la signature pour vérifier que c'est bien un message de Gépégix.

Dans l'autre sens Pégépa couvre son message de Publix vert et signe avec un peu de Privada orange.

Ainsi une fois que chacun au conseil des druides a composé ses deux potions personnelles, une privée et une publique, et qu'il dispose d'un exemplaire de la potion publique de chacun des autres druides, tout le monde peut échanger de façon sécurisée.

Crédits

Gepegix, by DragonOfTheFire, CC BY-NC-SA, https://dragonofthefire.deviantart.com/art/Farrous-Dathur-Air-genesi-324942566
Pegepa, by DragonOfTheFire, CC BY-NC-SA, https://dragonofthefire.deviantart.com/art/wood-elf-druid-201500166
Druid and Bear, by BentheBeard, CC BY-NC-SA, https://benthebeard.deviantart.com/art/Druid-and-Bear-184216690
Djin girl, by Riff, CC BY, https://www.sketchport.com/drawing/4871174758596608/a-hedge-djinn
Djinn, by Riff, CC BY, https://www.sketchport.com/drawing/4871174758596608/a-hedge-djinn
Pink Djinn, CC0, http://www.publicdomainpictures.net/pictures/180000/velka/genie-and-lamp.jpg
Scroll, by Hydroxonium, CC BY-SA 3.0, https://commons.wikimedia.org/w/index.php?curid=17440648
Splatter, CC0, https://pixabay.com/p-312092
Potion, CC0, https://pixabay.com/p-576862
Broomstick, CC0, https://pixabay.com/p-1297877
Maze, CC0, https://pixabay.com/en/maze-game-lost-map-confused-play-48698
Wizard, CC0, https://pixabay.com/en/wizard-magic-scroll-mage-magician-1456914
Troll, CC0, http://www.publicdomainpictures.net/view-image.php?image=177686&picture=troll-21

picasoft

CC BY NC SA

http://picasoft.net

Gépégix et le labyrinthe de Tor
(une métaphore du réseau d'anonymisation Tor)

Il reste encore un problème à Gépégix, il s'est aperçu que pour surveiller ses agissements, des chefs de clans ou des bandits de grand chemin surveillaient ses échanges.

Grâce aux potions, ils ne peuvent pas savoir ce que contiennent ses messages mais ils peuvent savoir avec qui il communique. Ainsi quand ils interrogent les messagers et qu'ils apprennent que des messages sont échangés avec Akaquarantesix spécialisé dans les sorts guerriers, ils se doutent que son clan prépare quelque chose de musclé ; quand c'est avec Pharmacix, ils se disent qu'une maladie est sûrement en train de sévir.

Les oracles sont de plus en plus exercés à découvrir ce qui se trame en fonction des messages échangés, même sans en connaître le contenu.

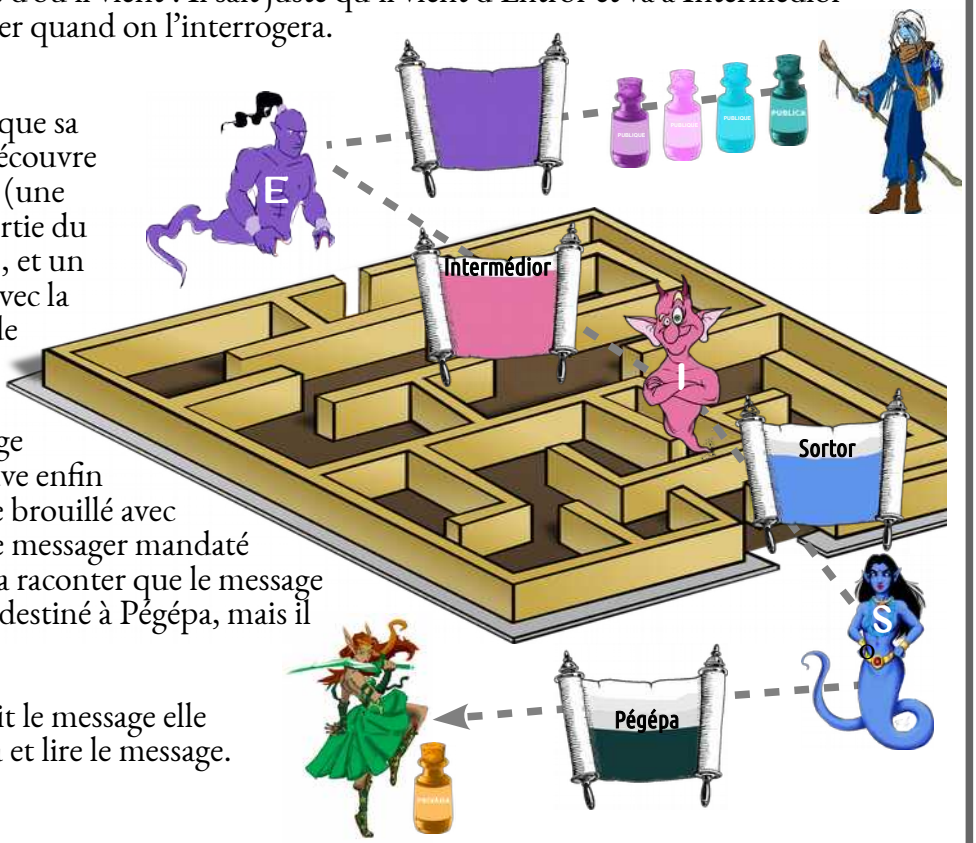
Alors Gépégix se coordonne avec des druides du monde entier pour créer le labyrinthe de Tor dont l'objectif est de masquer la provenance et la destination des messages.

Quand Gépégix veut communiquer avec Pégépa, il envoie un message à Entror, un djinn situé à l'entrée du labyrinthe de Tor. Bien sûr, Gépégix a brouillé son message avec la potion Publicor d'Entror, donc seul Entror peut le lire. Ce message contient l'adresse d'un second destinataire, Intermedior, et un autre message brouillé avec la potion d'Intermedior.

Donc Entror ne peut pas lire le message (puisqu'il est brouillé avec la potion d'Intermédior), mais il peut le lui transmettre, puisqu'il a déchiffré son adresse avec sa potion privée.

Le messager qui transmet le parchemin entre Entror et Intermédior ne peut toujours pas lire le message, mais il ne sait même plus d'où il vient ! Il sait juste qu'il vient d'Entror et va à Intermédior et c'est tout ce qu'il pourra raconter quand on l'interrogera.

De la même façon Intermédior applique sa potion privée et découvre l'adresse de Sortor (une djinn située à la sortie du labyrinthe de Tor), et un message brouillé avec la potion publique de Sortor.



Sortor quand elle reçoit le message applique sa potion privée et trouve enfin l'adresse de Pégépa et un message brouillé avec la potion Publica de Pégépa. Si le messager mandaté par Sortor est intercepté il pourra raconter que le message vient du labyrinthe de Tor et est destiné à Pégépa, mais il n'en saura pas plus.

En revanche, quand Pégépa reçoit le message elle peut appliquer sa potion Privada et lire le message.

Grâce au labyrinthe de Tor il devient très difficile de savoir d'où viennent et où vont les messages, les oracles sont bien embêtés pour essayer de deviner les activités des druides, et ceux-ci sont plus tranquilles pour échanger librement.

CC BY NC SA