       - la méthode Échange de clés Diffie-Hellman avec le lien suivant : https://fr.wikipedia.org/wiki/%C3%89change\_de\_cl%C3%A9s\_Diffie-Hellman

       Assez facile à comprendre on va pouvoir donner un exemple dans le rapport et il donne le moyen de contrer ce procédé en se mettant au milieu de la communication mais si les messages sont signés on ne peut pas agir.

   - Pour ne pas compromettre adresse IP le client ne peut pas faire de requête DNS donc cette requête est effectuée par le Noeud de sortie qui ne connait pas le client ni le nœud Gardien. Cela est vrai que pour les adresses classiques par pour les Hidden services (service cachés)

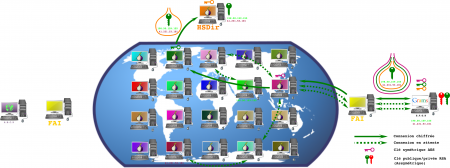
      - Pour les services cachés :

                -service caché va établir plusieurs circuits

                - récupérer ip des Noeuds de sortie qui vont servir de Pt d'introduction



               - services cachés demande maintenir connexion aux pt d'intro



               - service caché dépose son descripteur (sorte de ID) dans Une HSDIR

                             \*ID est composé de : -IPs pts de intro

                                                                - clé pub du service caché

                                                                - signature de tout ca avec la clé privé (il signe son message)

HSDIR = relais tor + info sur services caché

On devient HSDIR avec le consensus

              - client contacte HSDIR après avoir trouvé IP de HSDIR dans consensus et télécharge ID (descripteur service caché)

              - client établie circuit aléatoire où nœud de Sortie sera pt de rdv

* Client dépose secret au pt de rdv pour permettre dans le futur d’identifier le service cahé
* Machine établit circuit aléatoire vers pt d’intro (dont ip récup dans HSDIR)
* Pt d’intro relaye info jusqua service caché
* Client Tor envoi au service caché :
  + - IP pt de rdv
    - 1ère partie Diffie-Hellman
    - Secret du pt de rdv
* Toutes les infos sont chiffrés avec clé pub du service caché(prise dans HSDIR)
* Protection avec 3 relais coté client qui épluchent et 3 coté service qui repluche
* Service caché contacte pt de rdv avec secret pour s’authentifier
* Client et service procède a la deuxième partie de Diffie 🡺 création clé AES permettant communication chiffré

SECURITE

 Exitmap et HoneyConnector deux procédés de scan des nœuds de sorties, qui sont les plus compromettant .

Exitmap permet de détecter les manipulations du traffic en établissant une connexion Tor vers un leurre controllé par le Torproject (En sécurité informatique, on appelle ça un “pot de miel”, référence à un véritable pot de miel pour pièger les insectes). On sait ce qu’on envoie dans le réseau, et on regarde ce qui arrive sur le pot de miel. Si le traffic a été modifié, alors ça veut dire que le noeud de sortie modifie les trames réseau.

Honeyconnector permet de détecter le sniffage passif du traffic (C’est à dire la récupération des information sans les modifier). Concrètement, on envoie via Tor un couple unique “identifiant/mot de passe” sur un pot de miel toujours controllé par le Torproject. Ensuite, si une tentative de connexion a lieu ulterieurement sur ce pot de miel, alors on sait que le noeud de sortie par lequel ce couple d’identifiant est passé l’a intercepté.

Service caché sérieux = pas de javascript