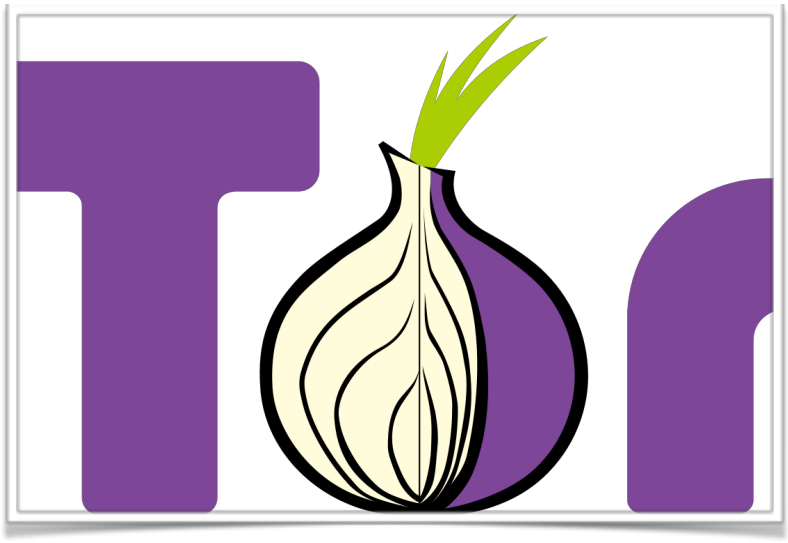
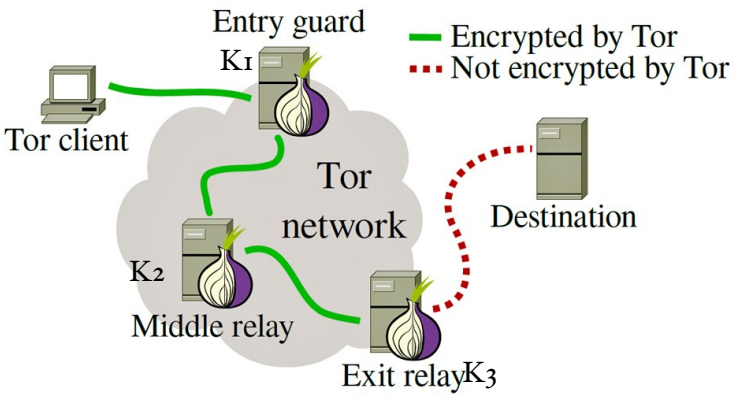


# How TOR works?

## It's open-source browser that is used to surf the web anonymously, now let's see how it works!

Like layers in onion there are layers of encryption and hops around the globe to fool the internet service provider and the government.

TOR(*The onion router*) browser uses the concept of onion routing which was developed by the US navy and it's different from virtual private networks, what it basically does is, it bounces the connection between multiple routers so that it becomes very hard to track and provides anonymity. The need of onion routing is important because sometime we don't even want people know that we have accessed something! Most of the communication we do is more or less based on client server architecture, tor provides us the ability to stay completely anonymous. So how those bounces or hops works, the onion routing bounces the connection multiple times with encryption between each hop with different keys from sender(tor user) to receiver(the server) and the last node on the path of hops actually communicates with the server(kind of a level one proxy) on behalf of the tor user along, how will seem to be communicating with an intermediate node which is nothing but a tor client only to confuse people about what's going on the route  from one end to another end.




The beauty of onion routing is that, on the network no-one knows anything about the while connection path **at a time a node only knows, from where the packet came and where to send it.**

And it also uses asymmetric encryption techniques like AES, and keys with each nodes are K1, K2, K3 exchanged using Diffie Hellman algorithm. Now as there are layers in onion here each layers has an encryption key. The message sent from the tor client is encrypted thrice with K1, K2, K3, Entry guard can peal the layer 1 with Key K1, and middle node can peal the encryption layer with K2 and so on bus at the last *Exit relay* the message is not encrypted anymore because it is nothing but a request for something to the server therefore it must not be encrypted and the *destination (the server)* replies to the message and the reverse process happens from K3 to K2 to K1 and the response can only be opened from the Tor client from which the original request came because it has the key *K1*.

There can be hundreds of nodes between the ends each can be in different countries also. But the main point is on each node the exit and tor client both must be using ssl because the only part that is not encrypted is that part only.

With all this encryption going on this browser is not the fastest! But it does what it's designed to do, *to make you anonymous and it does it pretty well!*