ECOLE
POLYTECHNIQUE
DE BRUXELLES

Communication Networks :
Protocols and Architectures
TOR Project

EL HALOUI Sami
KUY Yannick
ORBAN Maxime

23 December 2022

Teacher :
DRICOT Jean-Michel

Université Libre de Bruxelles
Ecole Polytechnique de
Bruxelles
ELEC-H417

Contents

1 Introduction

The TOR protocol is a research project introduced by the US Army in the 90s. It relies on enabled circuit-based of anonymous connections. The structure relays on a pool of relays that connects a client to its destination. Its major property is the mobility of the signal through the network and its encryption as every signal is encrypted each time it goes through a node within this pool. In this project, the main idea is to create a peer-to-peer network, where a client will connect anonymously through a network and send a message to the destination (like a TOR protocol), and a traditional peer-to-peer network.

2 Architecture of the Project

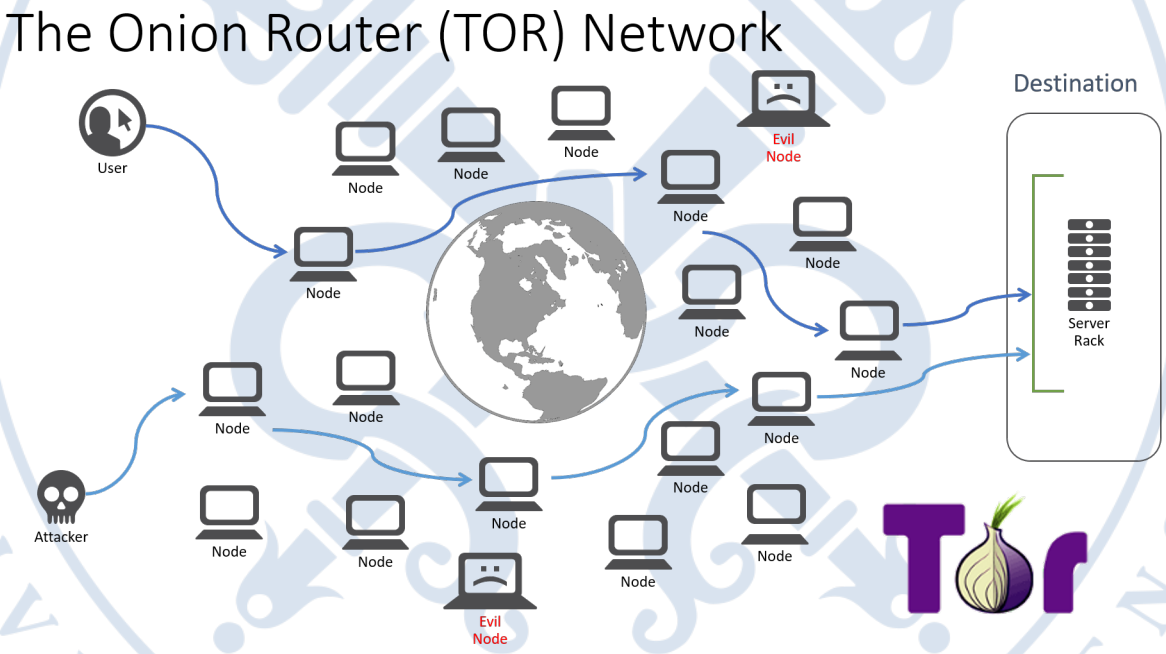

Figure 1: The Onion Router Network

A TOR network is made by nodes that are linked to each other, and one server that manages all the nodes through their addresses.

To send a message to the destination, the client will select 3 nodes randomly from the network. Then he will select one public key for each node in some order, and encrypt the message with each public key in the same order. Each node that receives the message will have the information of what node he must send the message to. This will

occurs until the final node sends the message to the destination. By this process, the destination can't easily retrace the path of the message and because in every node the message is encrypted, any observer of the network can't find the message.

3 Encryption

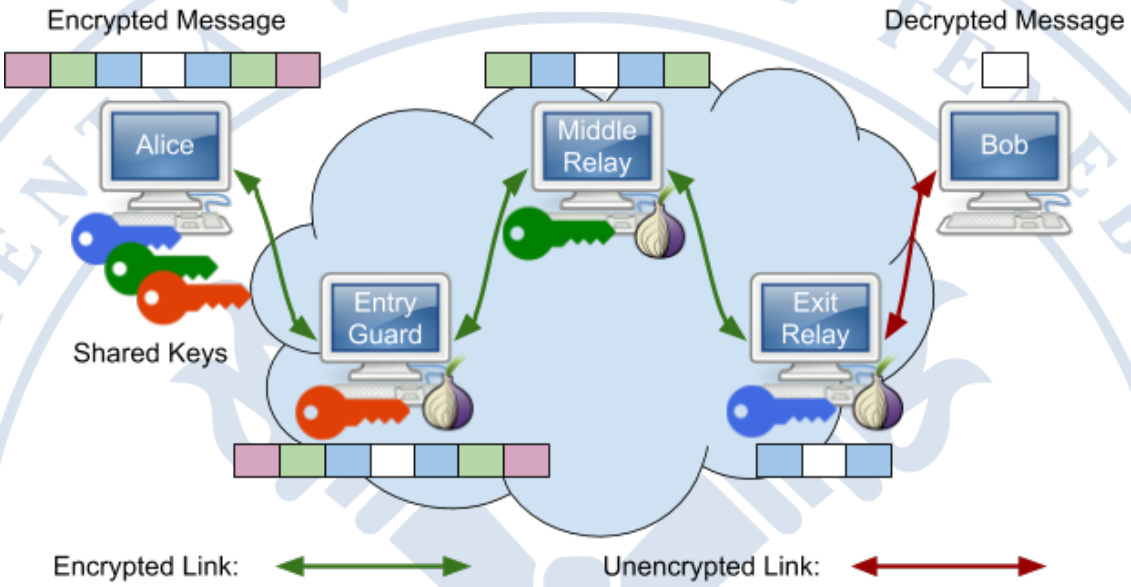

Figure 2: Encryption for TOR[2]

One of the pillar of this project is the encryption of the data. Each node contains a private key which means that the message must go through all nodes to be entirely decrypted. That's why the TOR Network is also called "Onion Network"

3.1 Asymmetric Key Encryption

The TOR Network requires a system of private and public key for each nodes to ensure its security.

That's why asymmetric key encryption was the first encryption techniques suggested. But this encryption has a weakness for the network : the encryption cost too much space for encryption encapsulation (it can only encrypt 190 bytes for a limited 2048 bytes used)

[2]https://medium.com/systems-and-network-security/tor-anonymity-for-better-or-for-worse-d8407b1d9287

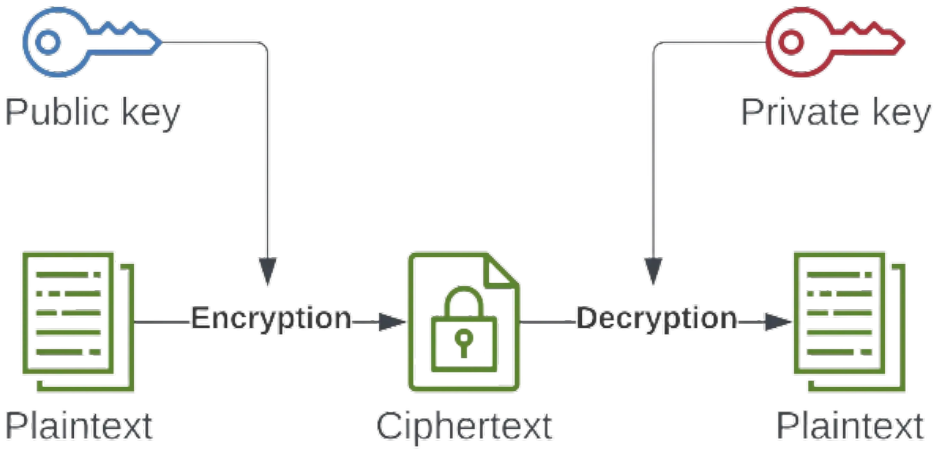

Figure 3: Asymmetric Key Encryption[1]

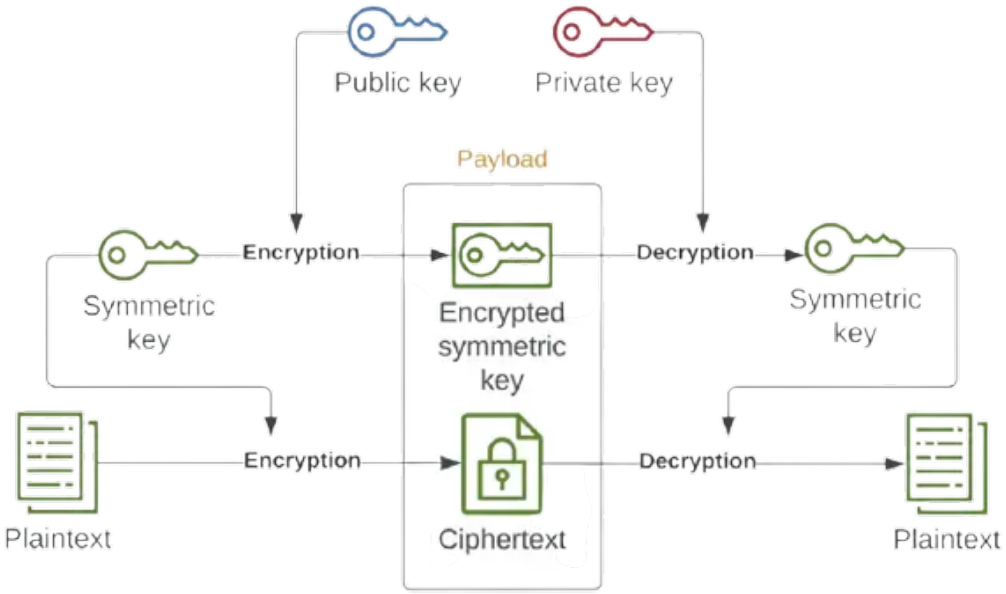

Figure 4: Hybrid Encryption[1]

3.2 Hybrid Encryption

The idea of hybrid encryption is summarised in Figure 4. The data is encrypted by a symmetric key and the symmetric key is encrypted by the public key of the receiver.

[1]https://medium.com/@igorfilatov/hybrid-encryption-in-python-3e408c73970c

The encrypted data and the encrypted key are sent to the receiver. The receiver will decrypt the symmetric key with his private key and he will decrypt the data with the symmetric key.

The advantage of this method is that it's more secure than symmetric key encryption because it has a system of public and private keys and it can encrypt more bytes than the asymmetric key encryption.

4 Libraries Python

The core tool used to simulate the network in this project is the socket library and each connection between sockets are represented by threads, there is only one socket by node. The library used for encryption is the cryptography library for python.

5 Challenges of The Project

- The choice for libraries were difficult because there were a lot and we didn't know where to start
- 2 choices could be make : code the network ourselves or take a library to do it for us. The first choice was made because the library used too many complex methods.
- The encrypted messages could be written in strings or in bytes, it leads us to misunderstand the state of the message.
- We took a lot of time (3h) to find the existence of hybrid encryption

6 Conclusion

This project taught us a lot about peer-to-peer network and encryption encapsulation. It also shows us different ways to be anonymous on the internet compared to the VPN we learned in the labs. It was also very fun to code.