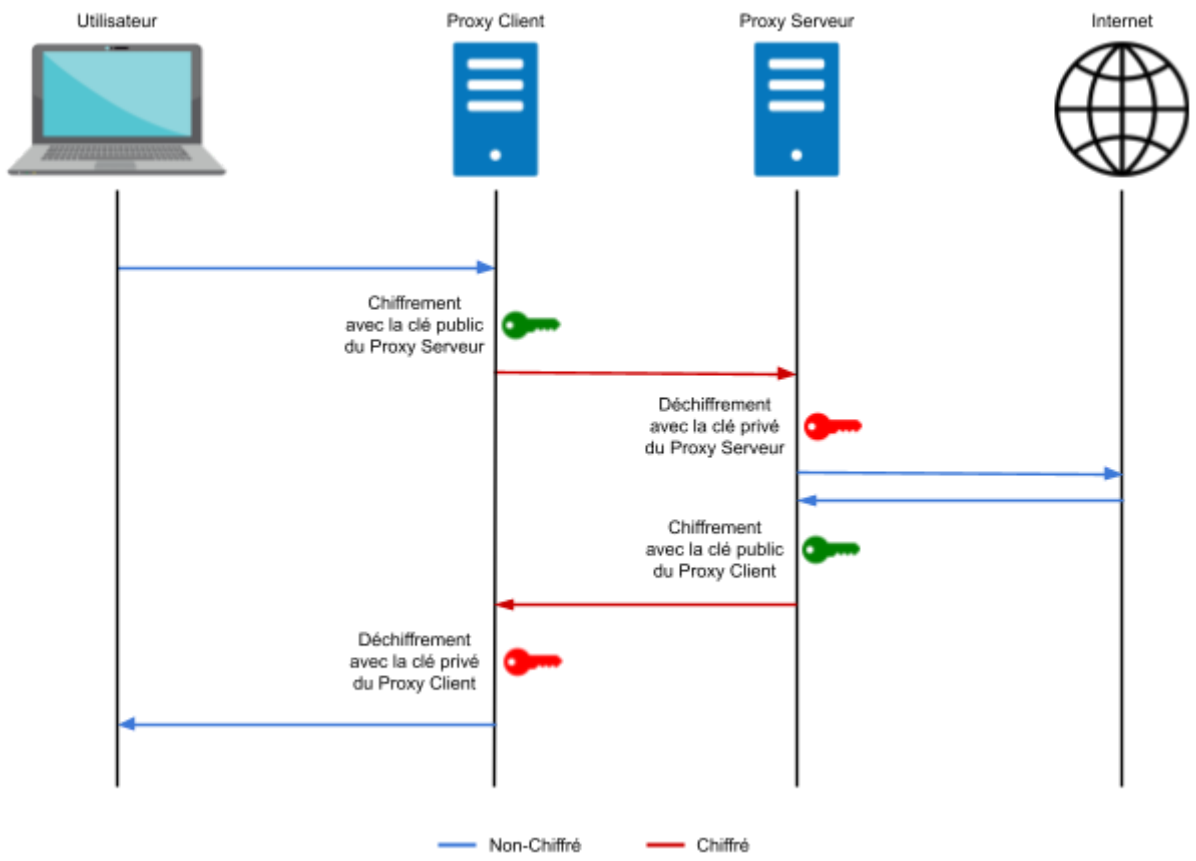
Github : https://github.com/M4verickFr/info731_proxy

Sujet : Les communications web peuvent être surveillées et écoutées. Afin de traiter ceci nous souhaitons mettre en place un mécanisme permettant de chiffrer le trafic à l'entrée d'un domaine ou le trafic est susceptible d'être écouté et de déchiffrer celui-ci à la sortie. L'objectif de ce projet est le développement de ce proxy. Le proxy reçoit les requêtes http issu d'un navigateur web qui a été configuré pour utiliser un proxy et chiffrer ces requêtes avant de les envoyer au proxy de sortie. Le proxy de sortie fait la requête http au serveur web à la place du navigateur web, reçoit la réponse la chiffre et la renvoie vers le proxy source, qui renvoie finalement au navigateur qui affiche la page demandée.

Outils : Sujet réalisé en nodeJS a l'aide du module ***net*** pour gérer les serveurs Proxy, ainsi que les modules ***fs*** et ***node-rsa*** pour le fonctionnement RSA. J'ai utilisé ***Chrome*** comme navigateur web avec l'extension ***SwitchyOmega*** pour indiquer au navigateur d'utiliser un proxy différent du système.

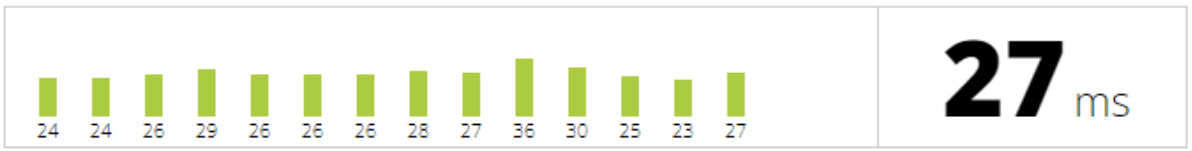
Fonctionnement :



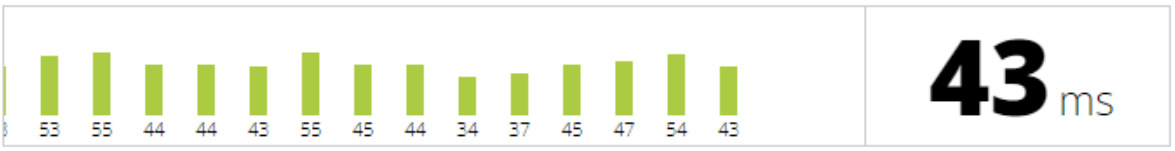
Performance :

Le proxy fonctionne sur un grand nombre de sites, celui-ci a été testé sur différents sites comme Facebook, Youtube, Google, DuckDuckGo, Github, Amazon, Le Monde et Apple.

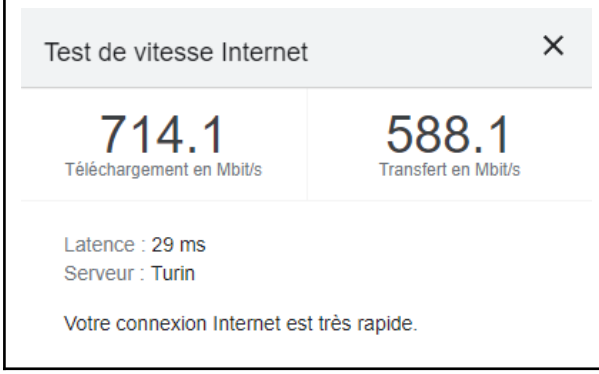
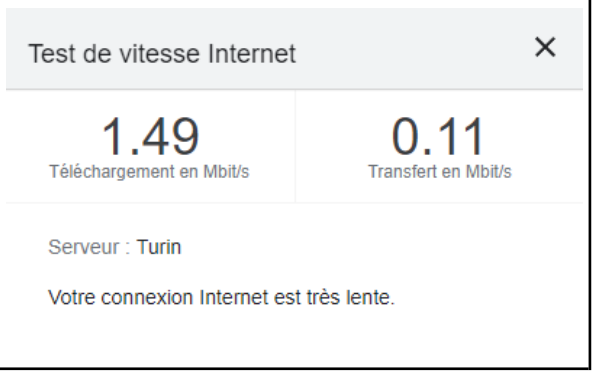
Délai sans le proxy :



Délai avec proxy :



Le délai (ping) est légèrement augmenté, mais cela ne cause pas de problème.

Sans le proxy	Avec le Proxy
	

Comme nous pouvons le voir ci-dessus, le proxy réduit considérablement le débit.

🛠 Installation

This project is intended to work with Nodejs, to install the project you need to clone the repository:

```
git clone git@github.com:M4verickFr/info731_crypto.git
```

Then install the dependencies:

```
yarn
```

And finaly generate RSA Keys:

```
node generateKeys.js
```

🕐 Quickstart

Starts proxies:

```
node serverProxy.js
```

```
node clientProxy.js
```

Then config your browser to use http://localhost:8080 as Proxy Server. I personally use **SwitchyOmega** extension on Chrome.