Initiation au chiffrement

Exemple avec la messagerie instantanée

Chiffrement ?

- On l’appelle aussi **cryptage**.
- C’est un **procédé technique** utilisé en informatique.
- C’est une technique qui vise à **protéger un contenu** d’une lecture standard en complexifiant la manière de lire un message.
- Seul là ou les personnes possédant **la clé de déchiffrement** sont habilités à déchiffrer le message.
- César lui même l’utilisait !

Pourquoi parler de César ?

- Lorsque César avait besoin de parler à ses généraux il leur envoyait un message. Eh oui, le smartphone n’existait pas !
- Ce message papier était codé avec une technique de chiffrement. Seul César et le destinataire possédait la clé pour déchiffrer ce message. Le messager ne pouvait le déchiffrer.
- César utilisait une technique simple qui consistait à décaler l’alphabet d’un certain nombre de lettres.

Un petit jeu

- Si je vous expose ce mot que me répondez-vous ?

irupdwlrq

Un petit jeu

- Et celui-ci ?

fmir nsyi

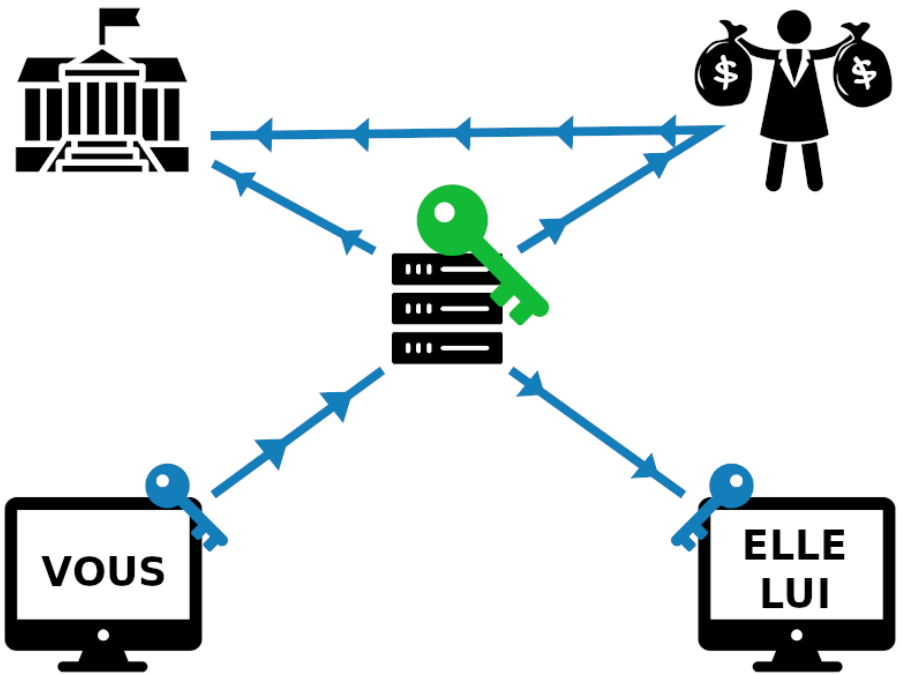
Solutions

- Le 1er mot était **formation** avec un décalage de 3 lettres vers l’avant.
- Le 2ème mot était **bien joué** avec un décalage de 4 lettres vers l’avant.
- Il existe de nombreuses façon de chiffrer un message cette technique permettait de protéger les communications entre les personnes.
- De nos jours nous n’utilisons presque plus le papier pour communiquer cependant nos messageries utilisent le chiffrement de manière transparente.

Les messageries instantanées

- Elles utilisent pour beaucoup le chiffrement cependant pour certaines ce n’est qu’un argument marketing.
- En effet la clé de déchiffrement n’était connu que de César et de son destinataire. Sur certains logiciels de messagerie la clé est stocké ni sur votre téléphone, ni sur celui du destinataire mais sur un serveur centralisé d’une entreprise privée qui potentiellement peut vendre vos données personnelles où se faire pirater.
- Peu rassurant n’est-ce pas ? Rassurez-vous il existe des solutions.

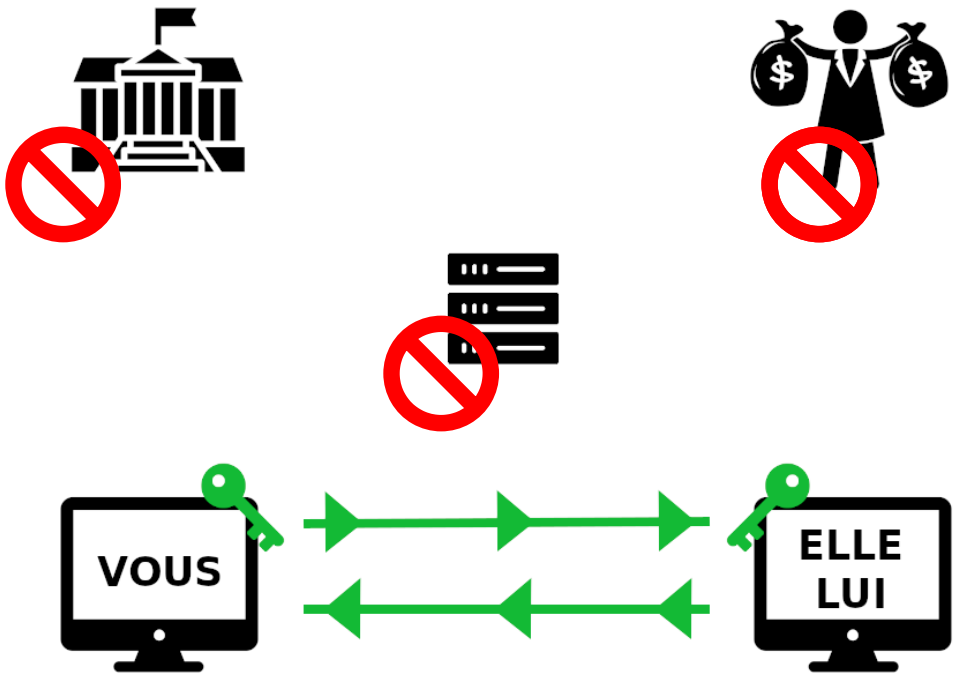
Un petit schéma pour illustrer ça



Fonctionnement centralisé

- En vert la **masterkey** du serveur qui permet de déchiffrer tous les messages
- Le publicitaire peut donc récupérer des données et les vendre
- L'état peut effectuer une surveillance
- L'internaute croit qu'il est protégé par le chiffrement

Un petit schéma pour illustrer le P2P



P2P signifie Peer to Peer ou Pair à Pair

- Chaque participant à la communication possède une clé de chiffrement.
- Il n'y à pas de serveur centralisé juste l'utilisation d'un logiciel.
- Vous remarquerez que c'est un schéma plus simple et donc consommant moins d'électricité, ce qui protège également l'environnement.

Le P2P et l’industrie

- Pour des industriels qui n’en ont rien à faire de l’environnement et qui souhaite récupérer vos messages pour les analyser ou vendre les données le P2P est un ennemi à la bonne tenue de leur business.
- Il y à aussi une raison technique. Il est actuellement plus compliqué de développer une application P2P qu’une application standard utilisant un modèle centralisée. Cependant le coût de développement, de maintenance, de la sécurité d’un serveur centralisé gérant les messages est gigantesque.

Des solutions P2P

Session est une messagerie utilisant un protocole P2P. Elle est moderne et dispose de toutes les fonctionnalités des plus connues.

Jami est crée par une entreprise Québequoise. Elle existe sur beaucoup de support et propose la plupart des fonctionnalités nécessaires.

Des solutions P2P

Retroshare est une plateforme extrêmement complète fonctionnant en P2P. Forum, Blog, Messagerie, Audio, Vidéo, Partage de fichiers tout y est.

TOX

Tox est un logiciel de messagerie instantanée proposant l’audio la vidéo le texte et les conférences.

Les logiciels libres

- Tous les logiciels cités au dessus sont libres ce qui signifie que n’importe quelle personne peut consulter la manière dont ils ont étés conçus.
- Cette opportunité garantie par la transparence un fonctionnement du logiciel en accord avec les valeurs des utilisateurs.
  - Protection de la vie privée
  - Gratuité
  - Partage de connaissance
  - Possibilités d’apprentissage

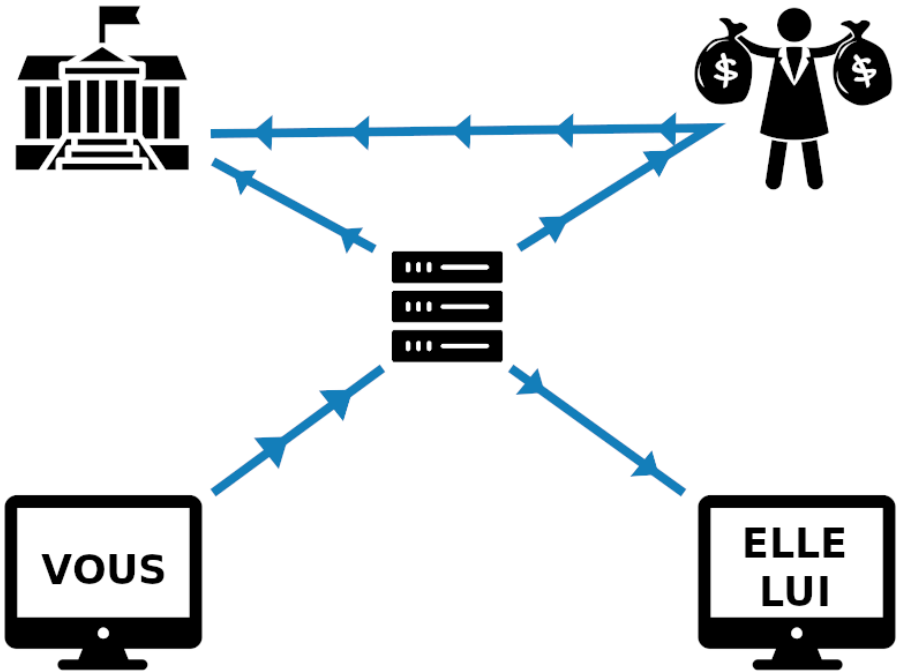
La masse critique

- Si le P2P « c’est bon mangez-en » comme on dit il ne faut pas nier que le marché actuel est surreprésenté par le modèle centralisé.
- La masse critique joue un rôle prépondérant dans cet état de fait. En effet qui est prêt à changer de messagerie si personne qu’il ou elle connaît l’utilise également ? Peu de gens, nous n’aimons pas être isolé et l’idée de se retrouver seul mais protégé n’est pas assez forte pour nous faire changer.
- Les gens qui changent le font souvent par curiosité scientifique ou engagement en faveur d’une cause (logiciel libre, vie privée, écologie).

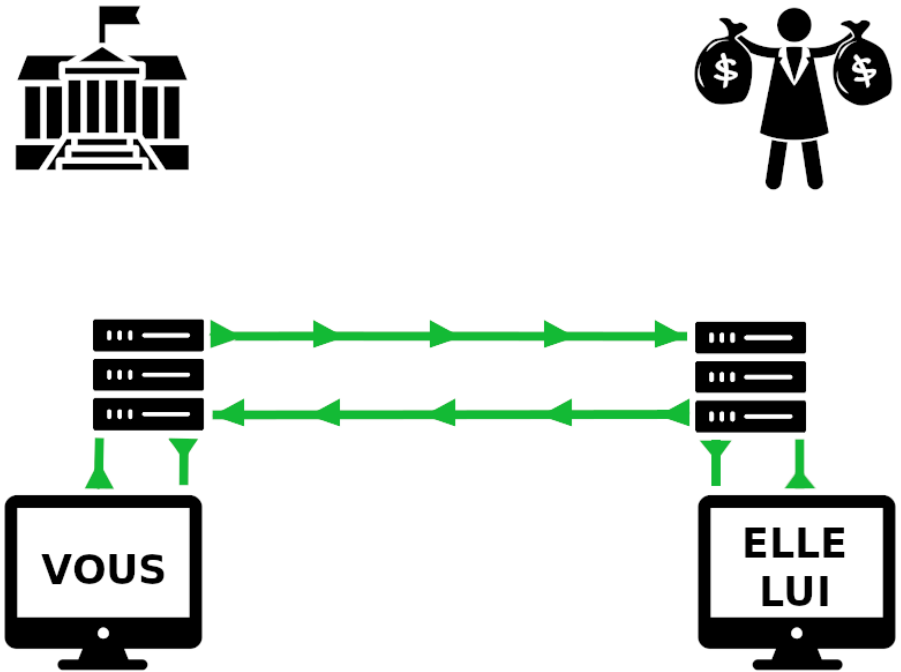
Alors tout est mal ?

- Non surtout pas il existe des logiciels utilisant d'autres méthodes que le P2P qui restent très bons.
  - **Conversations** sous Android
  - **Quicksy** sous Android
  - **Jitsi** qui est multiplateforme
  - **Rocket Chat**
  - **Mattermost**
  - Etc
- Il en existe beaucoup qui fournissent des services centralisés ou fédérés qui protège la vie privé.

Centralisé ou Fédéré

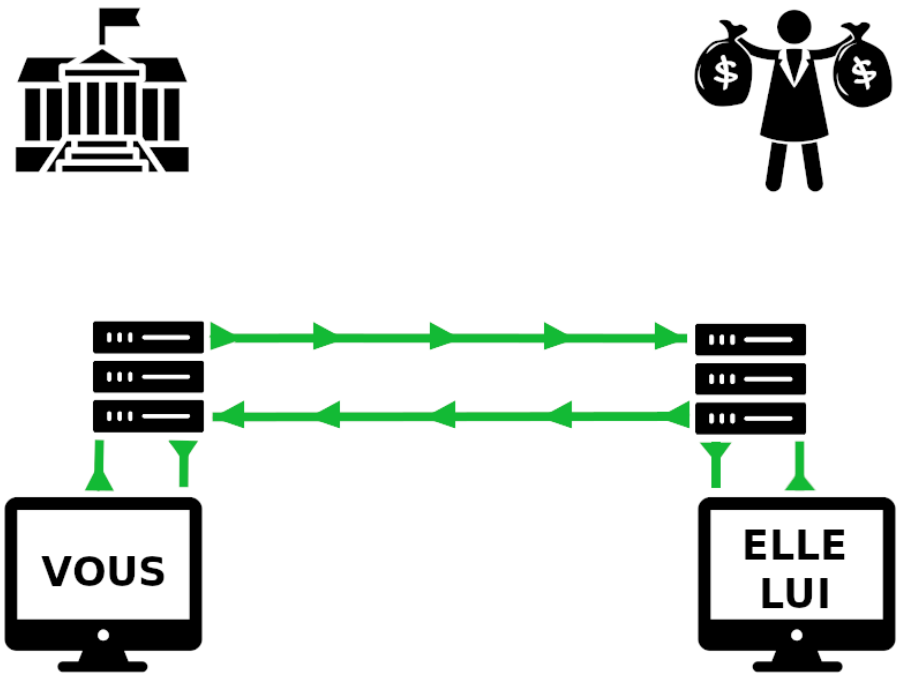


Centralisé



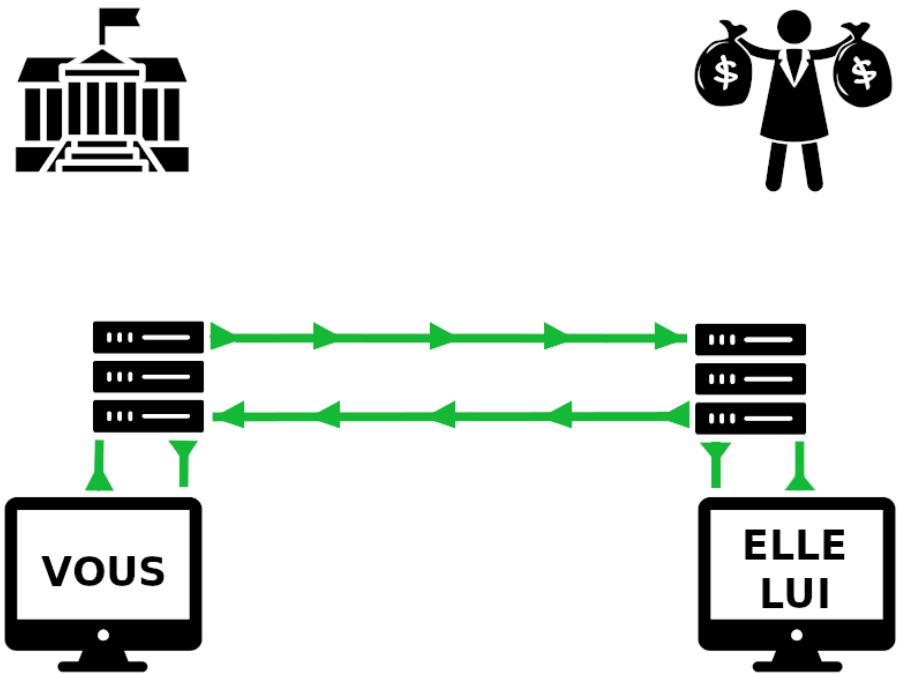
Fédéré

Explication du serveur fédéré



- On constate que dans le cas du serveur fédéré ce ne sont pas les ordinateurs qui communiquent directement mais les deux serveurs associés aux ordinateurs.
- Ces serveurs peuvent être soit individuels soit regrouper plusieurs personnes.

Explication du serveur fédéré



- La possibilité de créer des serveurs est laissée à l'utilisateur.
- Les différents serveurs se reconnaissent et échangent entre eux directement.
- Si un serveur est compromis il peut être isolé. Les serveurs communiquent ensemble seulement lorsque cela s'avère nécessaire.

Je suis perdu. Des logiciels à éviter ?

- Malheureusement si vous souhaitez protéger votre vie privée la plupart des grandes entreprises sont à éviter :
  - **Américaines :**
    - What’s App, Facebook Messenger, Instagram, Snapchat, Skype, Hangouts, Duo, Google
  - **Chinoises :**
    - Tik Tok, Wechat, QQ, Kakao, Baidu
  - **Russes :**
    - Vkontakte, Yandex

La législation

- Les Etats cités au dessus ont soit demandé aux créateurs des applications de fournir les clés qui permettent de déchiffrer les communications soit ont inscrit dans leur constitution l'obligation de toute entreprise de leur territoire à partager toutes les communications.
  - Cette loi s'apelle le **Patriot Act** aux Etats Unis.

Je m’en fiche j’ai rien à cacher

- C’est une position que l’on entends souvent. Si vous n’avez rien à cacher peut être que quelqu’un dans vos contacts à quelque chose à cacher. Des données de santé, des préférences sexuelles ou politiques. En utilisant certains logiciels vous communiquez parfois les informations d’autres personnes, pensez-y.
- Le but n’est pas de faire culpabiliser même si cela peut en prendre la forme mais avant tout d’informer et de sensibiliser pour que le jour où quelqu’un de votre entourage changera de pratique vous puissiez faire votre propre choix éclairé grâce à votre recul technique.

Un dernier mot

- Vos habitudes et vos pratiques sont à la fois votre force et vos faiblesses. L'habituation à des pratiques délétères par l'utilisation sans recul de différentes applications peut mener à des résultats non souhaités par l'utilisateur (SPAM, ciblage publicitaire)
- Malgré tout nous restons des êtres sociaux qui ont besoin d'être en contact les uns avec les autres d'une manière ou d'une autre. L'utilisation des logiciels où une masse critique est présent est donc nécessaire pour se tenir au courant ou rester proche. Cependant dans ce dernier cas rien n'empêche de changer tous ensemble.