Sécuriser ses communications

Comment sécuriser ses communications sur Internet ?

Présenté par:
Kayode DA CRUZ et Younoussa SOW

Plan

- Pour qui ?
- Comment ?
  - Sur le web
  - Le mail
  - Les messageries instantannées
- Quelles sont les limites ?
  - Législatives
  - Techniques

Pour qui ? Glenn Greenwald

- Je suis journaliste, je protège mes sources

« Si j'ai pu maîtriser le chiffrement de données, alors tout le monde peut le faire »

Pour qui ? Hillary Clinton

- Je suis une personnalité politique

Monde

Le piratage de la campagne d'Hillary Clinton par la Russie exige une réponse

Fred Kaplan — Traduit par Bérengère Viennot — 14 décembre 2016 à 13h48 — mis à jour le 14 décembre 2016 à 14h55

L'avenir de la démocratie et des relations internationales Est-Ouest est en jeu.

Pour qui ? Snowden

- Je suis un lanceur d’alerte

Pour qui ? Pour moi aussi

- Et pour tout le monde
  - Avocat
  - Médecin
  - Citoyen lambda

Pourquoi ?

- Confidentialités multiples, secret professionnel, vie privée et intimité
  - Secrets non liés aux personnes : négociations, finances, justice
  - Secrets liés aux personnes : vie privée, intimité, sentiments, famille

Contre qui ?

- Notre FAI
- Notre voisin: proche ou éloigné
- Les GAFAM, mais pas que…
- Les pirates
- Les “Cambridge Analytica”
- Les États
- Les régis publicitaires

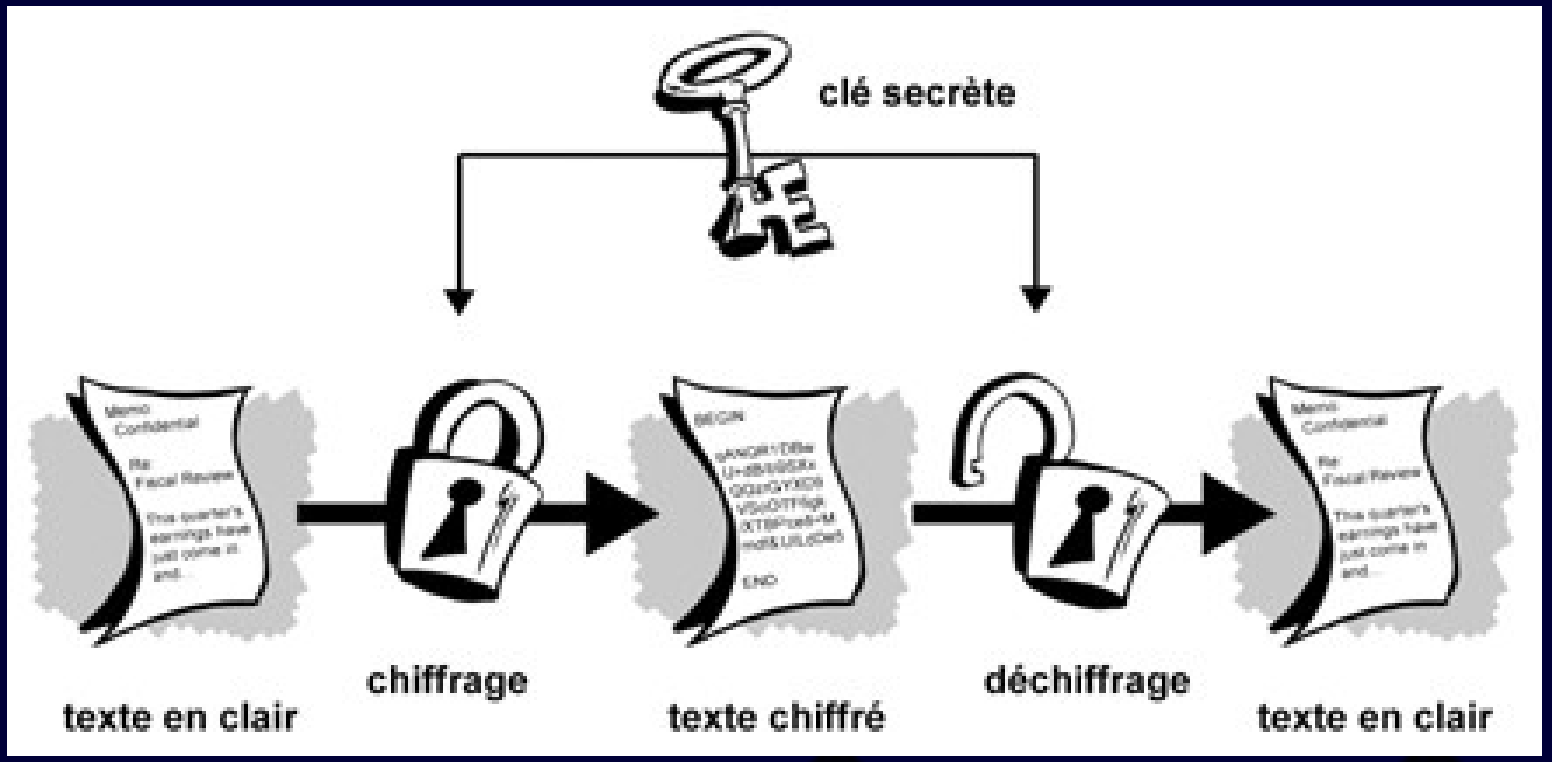
Comment ?

La solution: **Le chiffrement**

- **Symétrique:** **AES**, **Serpent**, Twofish, RC6, RC4, CAST, IDEA, DES, TripleDES, REDOC 3.
- **Asymétrique:** **RSA**, Diffie-Hellman, DSA (DSS), **ECDSA**, ECDH.

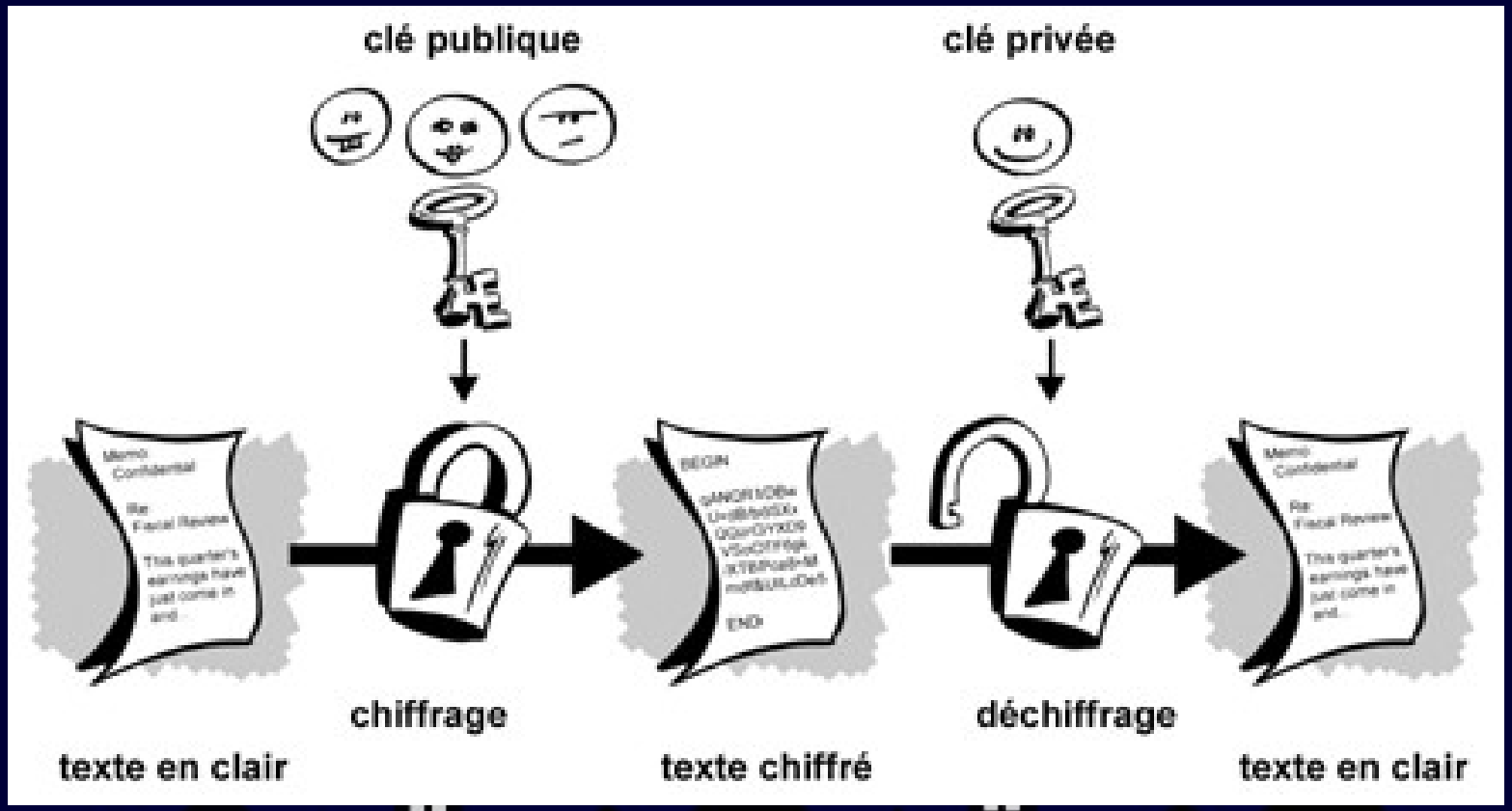
Les méthodes de chiffrements

- Le chiffrement symétrique
  - Principe de base : le cadenas, et la clé du cadenas



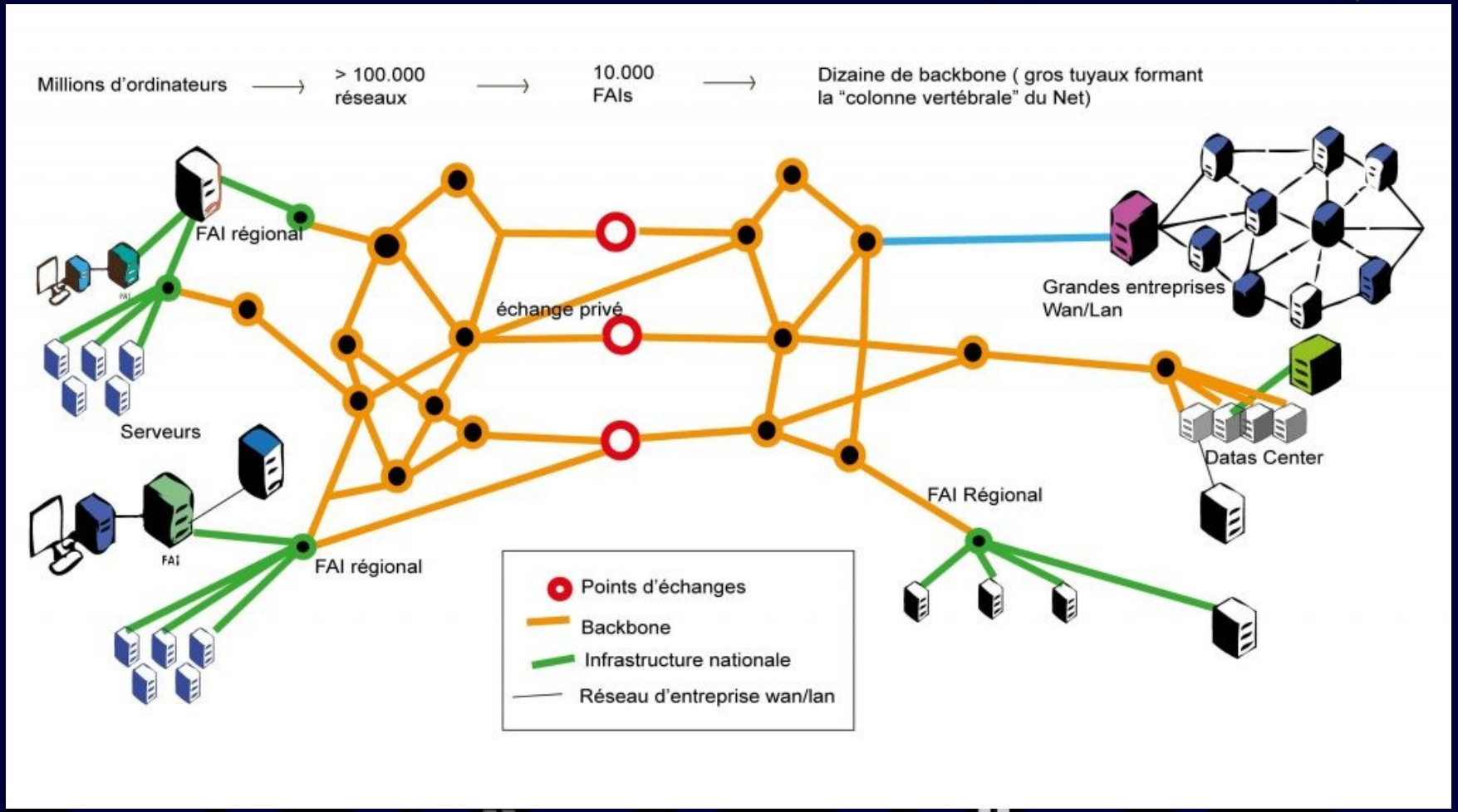
Les méthodes de chiffrements

- Le chiffrement asymétrique
  - Principe de base : les cadenas, et la clé des cadenas



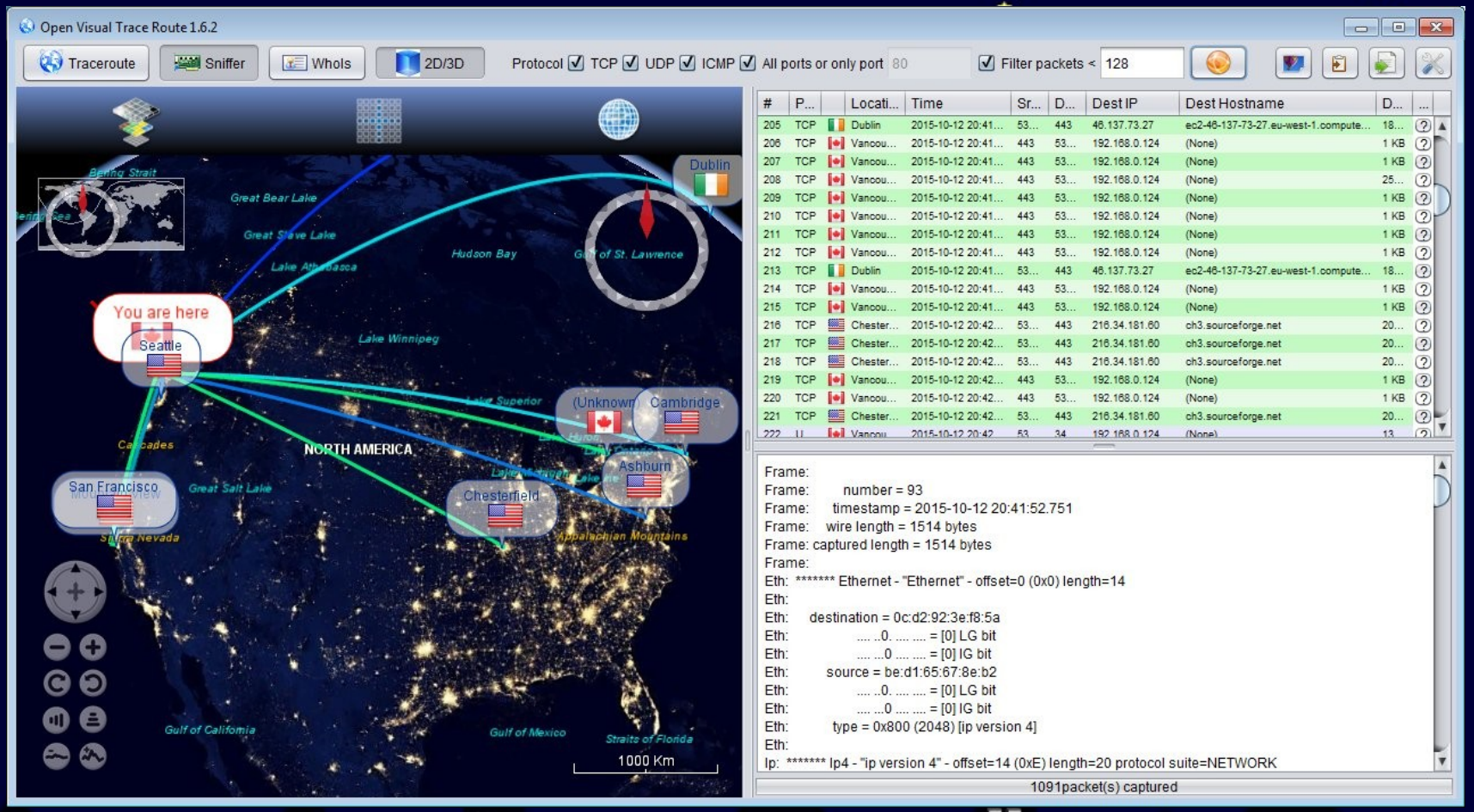
Rappels

Fonctionnement d’internet



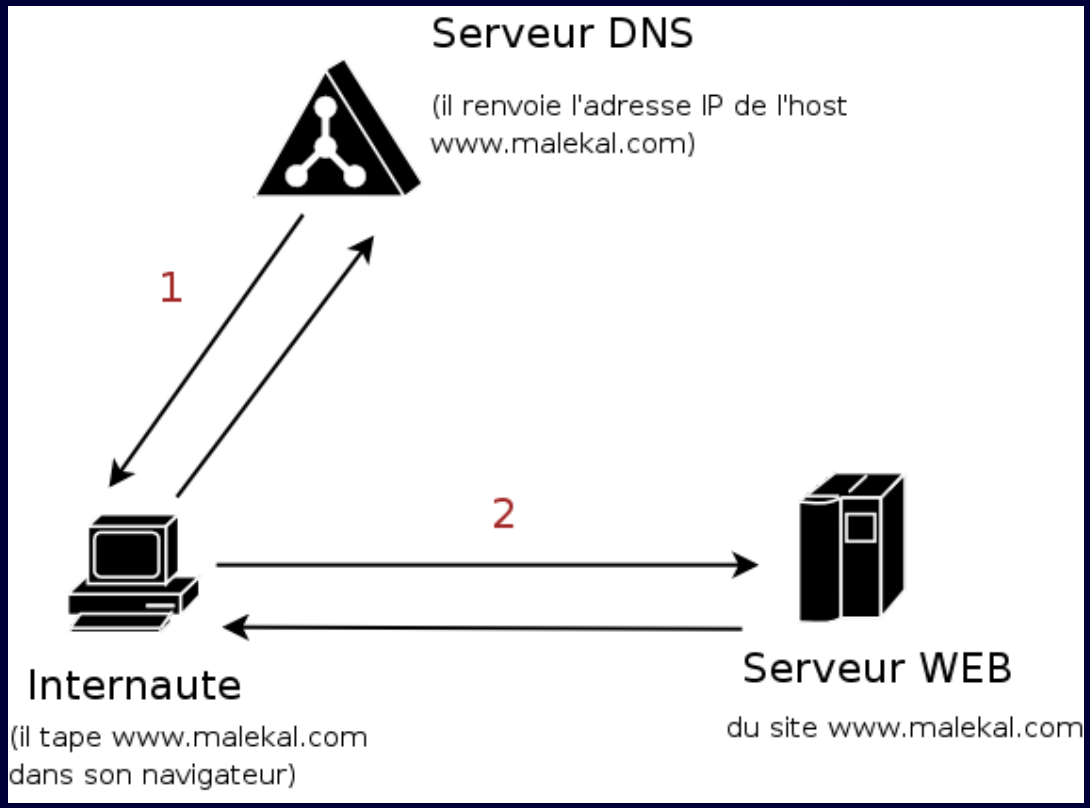
Rappels

Fonctionnement d’internet



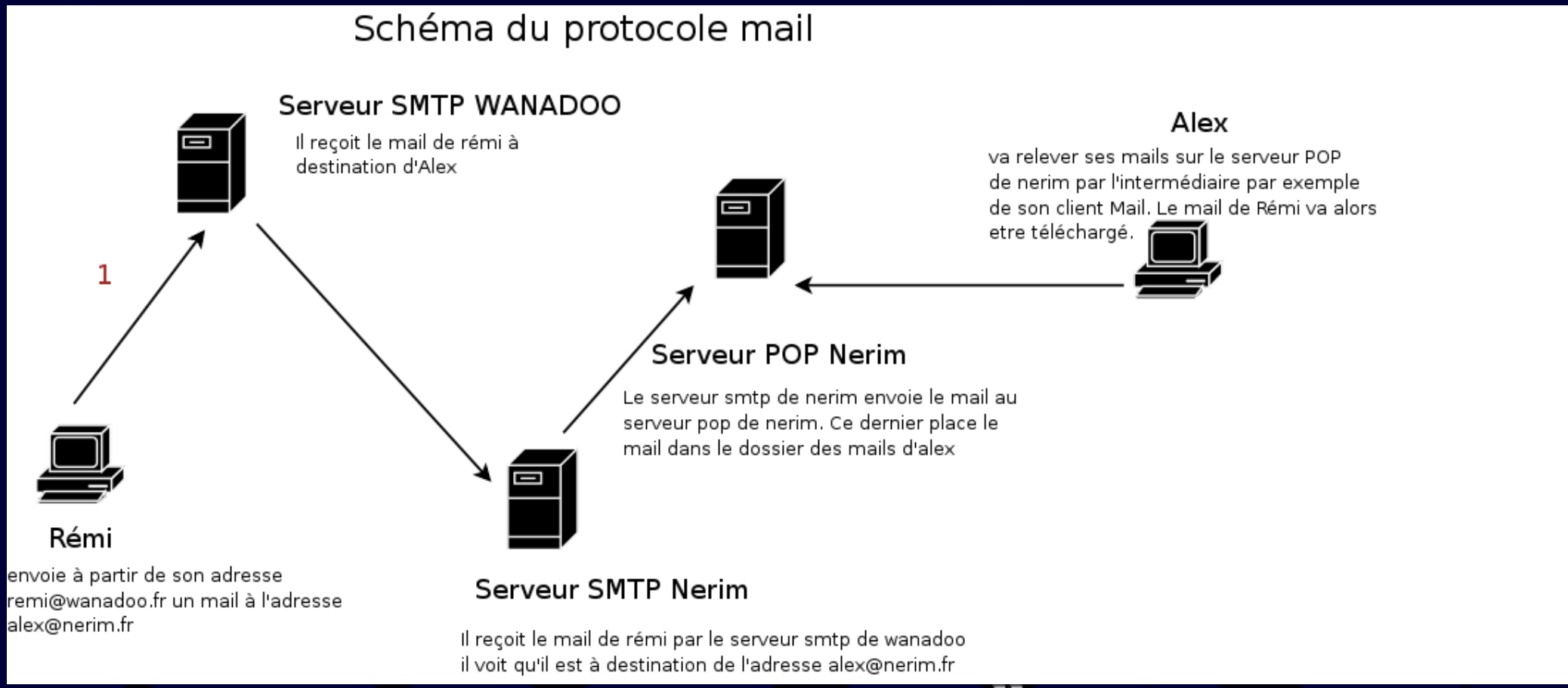
Rappels

Connexion à un site web



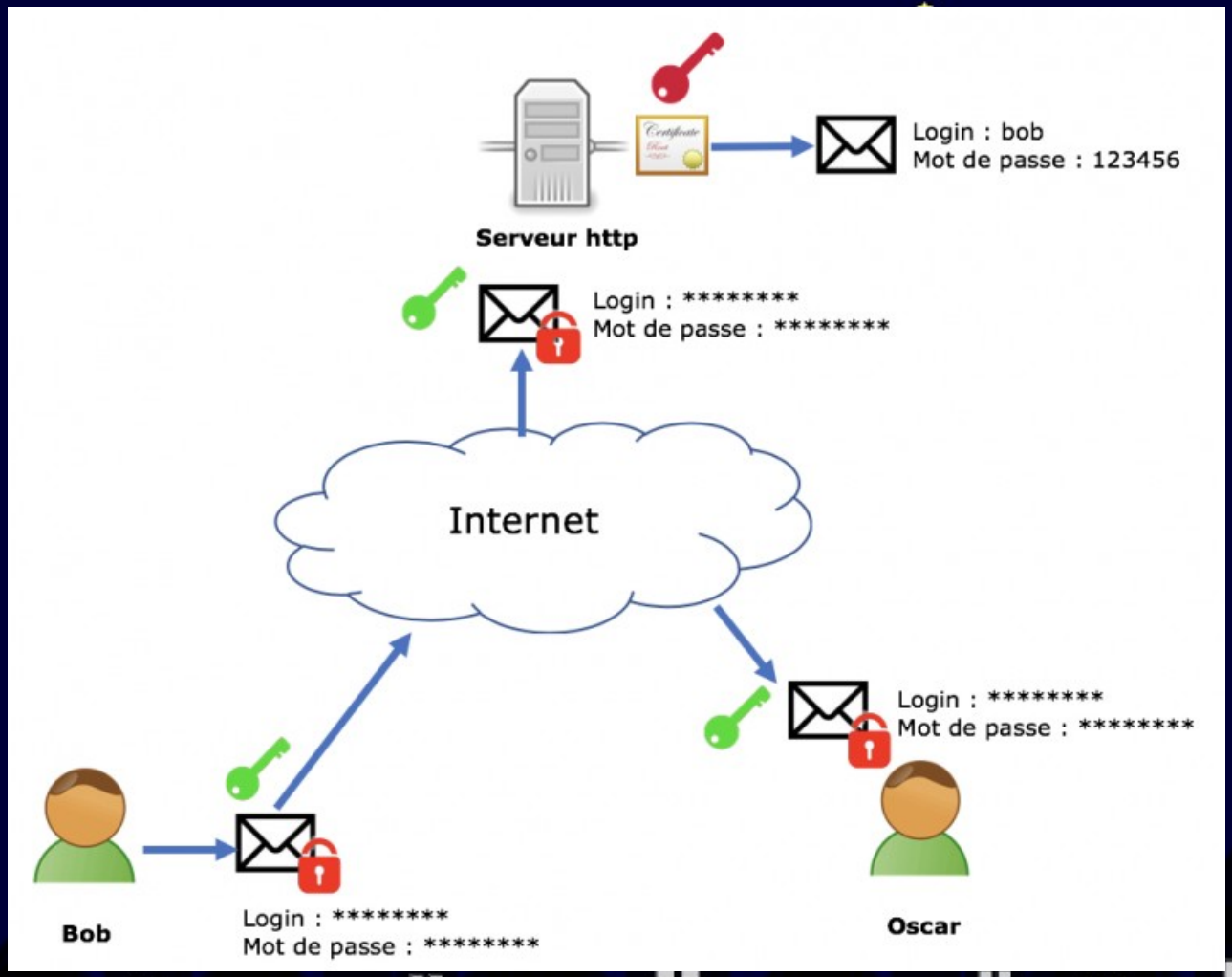
Rappels

L’envoi d’un mail



Les solutions

- Sur le web, surfez couvert: HTTP + ~~SSL~~ TLS



Les solutions

Pour le mail: utilisez GnuPG (Gpg4win)

- Client webmail + Mailvelope
- Client mail + Enigmail
  - Thunderbird
  - Outlook

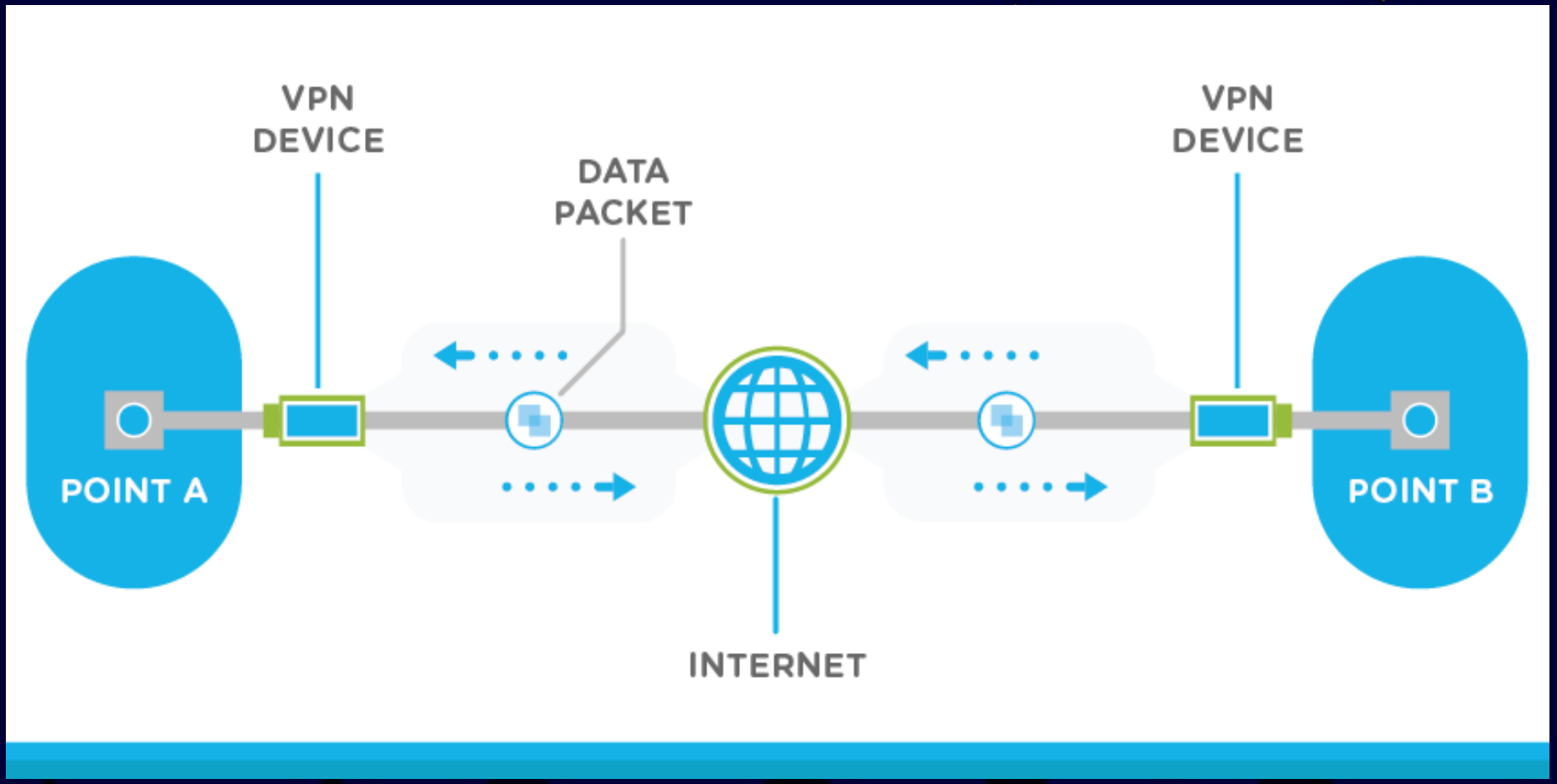
Les solutions

Le chat: Le chiffrement de bout-en-bout

- OTR + Xmpp : pour rester libre
  - Mobile : conversations, chatSecure
  - Desktop : pidgin, adium
- Signal au lieu de iMessage, ou SMS
- Whatsapp

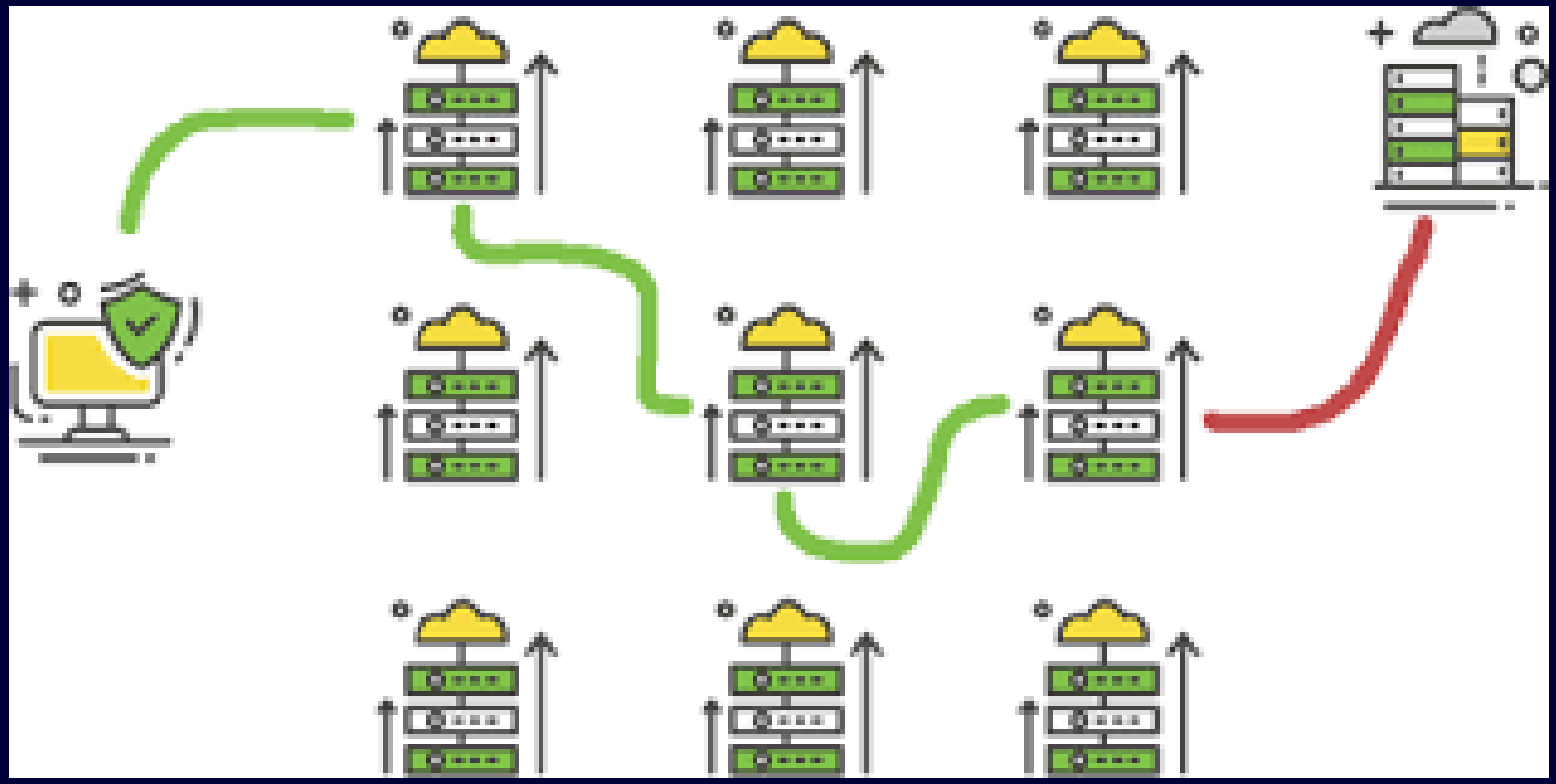
Proxy et VPN

- Pour l’anonymat



TOR

- Pour l’anonymat



Les limites

- La sécurité au dessus de la vie privée
- La complexité de la mise en œuvre
- Le fameux “je n’ai rien à cacher”
- Les questions éthiques
- Le manque d’informations

Conclusion

“Un peuple prêt à sacrifier un peu de liberté pour un peu de sécurité ne mérite ni l'une ni l'autre, et finit par perdre les deux.”

Benjamin Franklin