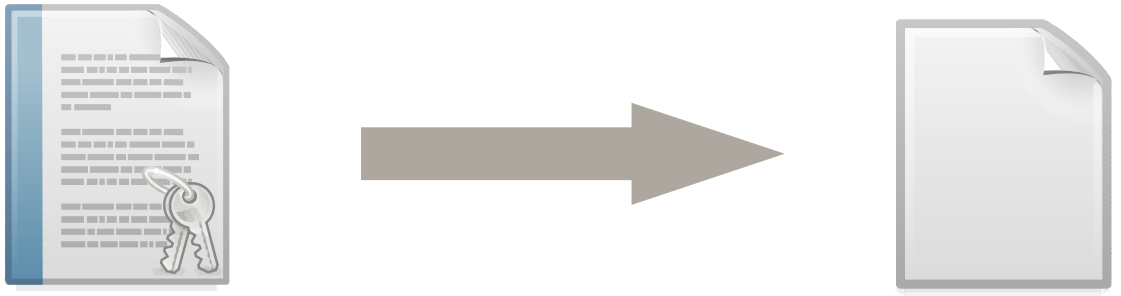
Chiffrofête – Partie théorique

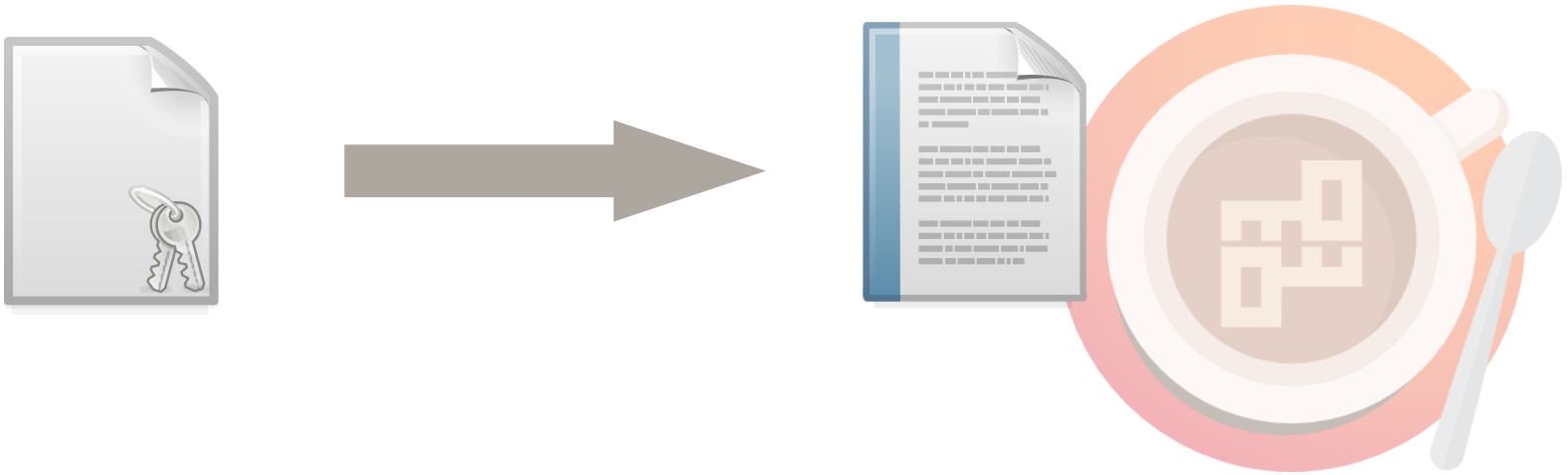
Sommaire

Vocabulaire technique

Chiffrer : Rendre un fichier illisible à l'aide d'un algorithme et d'une clé



Déchiffrer : retrouver le fichier original à l'aide de la clé



Différents types de clés

Exemple de mot de passe

```
baseball4673
```

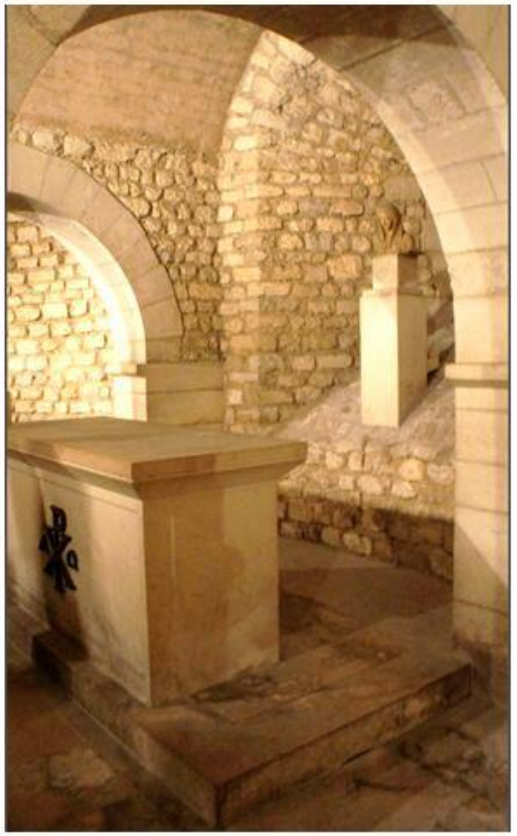
Exemple de phrase de passe

```
livre avion clavier quarante
```

Exemple de clé RSA

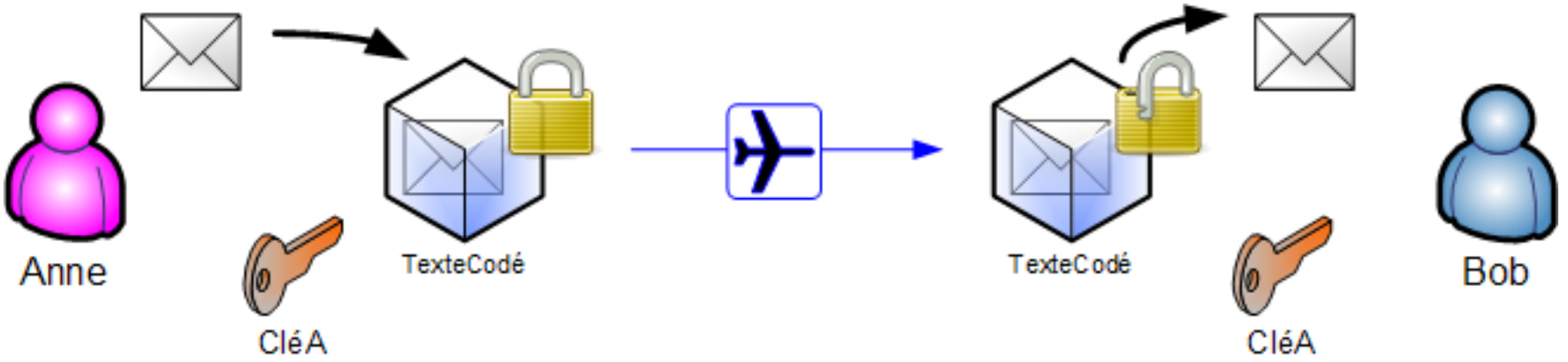
```
AAAAB3NzaC1yc2EAAAADAQABAAABAQDTvtEgjVBkfq6NmLHtlwtAtusCw3XIL947GowUzG
DnBLI565N8PMeJ/q5gKqPS/V56HIy2qPtzdH0hDXQ+cHcmThhx84xGh+Q+P95rLMo51wjK
sJ7hELbJg060CTno9oHJIeF0LKltm0k0lQSVOdofqD7jDhNwFZcap6MiRuB1+4nTto9tbq
S1tf1mmTShkC+F9uO/SrnPGYagMuPU+6Mzdv95h5z0UPUuOuiT0B4mt5zSTPN85Fdq5Z22
Ee4AceC19AS7yOpx7AByeh1SdgsuKgl083iCDUEfG4myFRuJ7CJk/MCvsZ42/ImwVsj8nP
Cy0NFkr8pYUYfTsuLXrFG3
```

Parlons en bon français

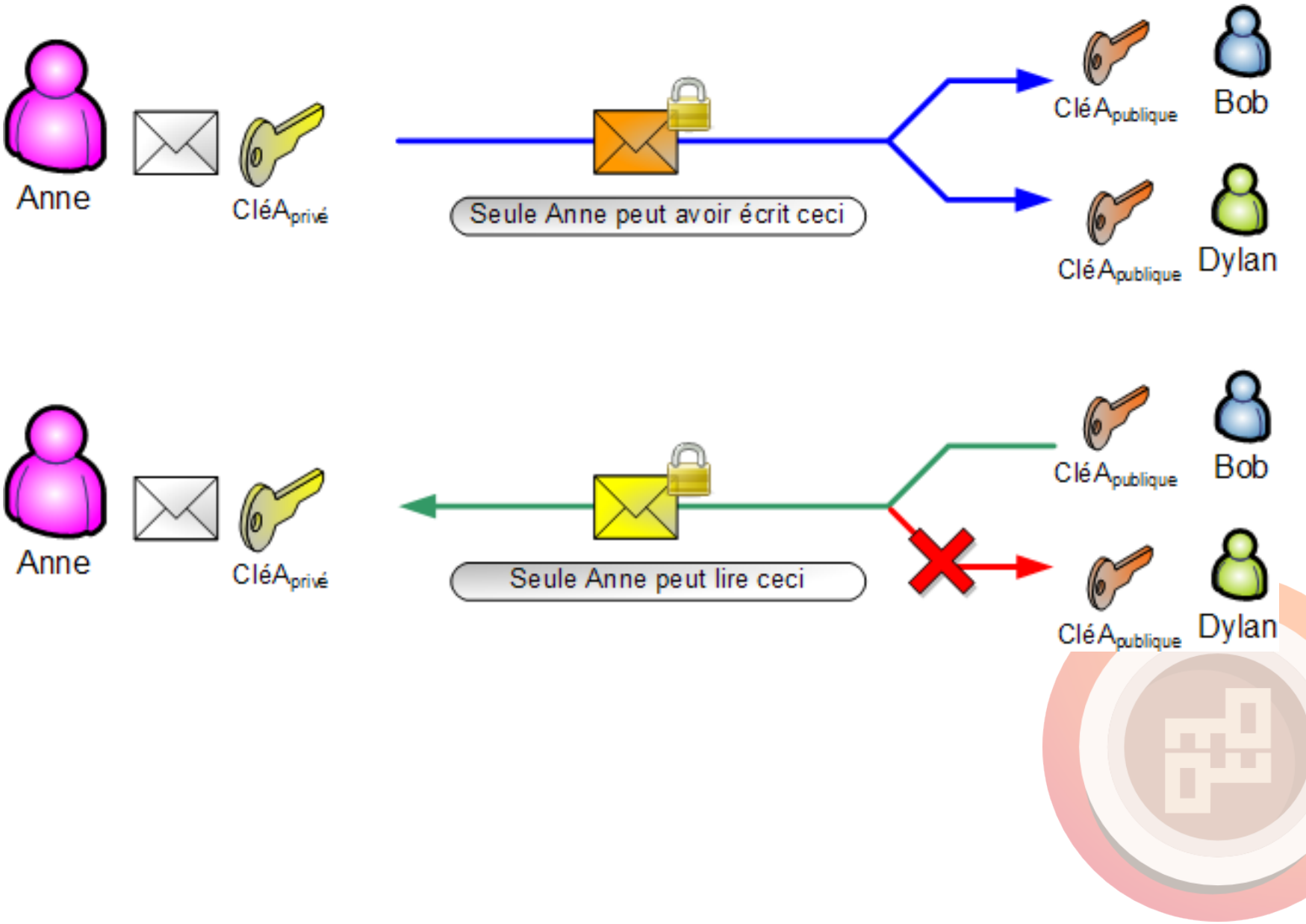


Mes données sont protégées, je les ai ~~cryptées~~ *chiffrées*.

Chiffrement symétrique



Chiffrement asymétrique : signer et chiffrer



Pourquoi chiffrer ses données

Parce qu'on ne se balade pas à poil dans la rue alors pourquoi sur le net ?

Parce qu'on veut se protéger des yeux indiscrets

Parce qu'on veut protéger sa vie privée

Parce qu'on a tous quelque chose à cacher !

Une démarche globale

Chiffrer ses données fait partie d'une hygiène numérique

Savoir pourquoi on chiffre ses données

Définir un modèle de menace

Comment protéger sa vie privée

Avec des logiciels libres de chiffrement

Truecrypt, dmcrypt, encfs, gnupg...

Avec des extensions de navigateur

µblock, AdblockEdge, Ghostery, WOT, HTTPSeverywhere...

Avec des proxy anonymes

TOR, I2P...

Avec des OS (systèmes d'exploitation) sécurisés

TAILS, la famille GNU/Linux, FreeBSD...

Avec du bon sens

Ne pas cliquer partout, faire attention à ce qu'on télécharge, maintenir son OS et ses outils à jour...

Pourquoi des logiciels libre

Logiciels libres = code source disponible = confiance

Ce que Genma nous dit :

Dès que possible, c'est le logiciel libre qui est privilégié.

Mais Apple, Windows et Android posent le souci de ne pas être des systèmes libres, donc on ne peut pas leur faire confiance.

Windows et Apple sont plus que fortement déconseillés dans le contexte de la confiance et de la crypto.

Faire de la crypto là-dessus, c'est un peu comme avoir une porte blindée à sa maison, mais avec des murs en carton-pâte.

Liens

Outils pour se libérer de PRISM - http://prism-break.org/fr/

Annuaire de logiciels libres - http://framasoft.net

Keepass - http://keepass.info/

TOR - https://www.torproject.org/

Truecrypt - http://www.truecrypt.ch/

Pour information le site web Truecrypt a été compromis.
Plus d'information chez Korben et Genma.

Merci de votre attention !

Merci de l'avoir regardé
N'hésitez pas à me faire des retour, ou des suggestions