

# Chiffrer ses e-mails avec GPG

## Présentation

Dans le cadre du *Festival des libertés numériques*  
12 février 2020

Leo Vivier

leo.vivier@gmail.com

C16 PGP

88A6 70C3 BAB2 FA14 F50D 7676 1D44 336A 099C 0A16



Ce document est mis à disposition selon les termes de la licence Creative Commons « Attribution - Partage dans les mêmes conditions 4.0 International ».

- 1 Introduction
- 2 Chiffrement symétrique
- 3 Chiffrement asymétrique
- 4 GPG : Explication

## 1 Introduction

- Objectif de la séance
- Bornes de la présentation
- Notes sur les outils utilisés pendant cette présentation
- Pourquoi chiffrer ses e-mails ?

## 2 Chiffrement symétrique

## 3 Chiffrement asymétrique

## 4 GPG : Explication

1. Ne pas se contenter de former à l'utilisation d'outils
  - Ce sera le but de l'atelier d'après (15h30)

# Objectif de la séance

1. Ne pas se contenter de former à l'utilisation d'outils
  - Ce sera le but de l'atelier d'après (15h30)
2. Approcher des concepts théoriques pertinents pour l'utilisateur lambda

1. Ne pas se contenter de former à l'utilisation d'outils
  - Ce sera le but de l'atelier d'après (15h30)
2. Approcher des concepts théoriques pertinents pour l'utilisateur lambda

## Postulat de départ

La compréhension superficielle de **concepts théoriques** liés à des **pratiques** mène à une utilisation plus *réfléchie* de leurs **outils**.

1. Ne pas se contenter de former à l'utilisation d'outils
  - Ce sera le but de l'atelier d'après (15h30)
2. Approcher des concepts théoriques pertinents pour l'utilisateur lambda

## Postulat de départ

La compréhension superficielle de **concepts théoriques** liés à des **pratiques** mène à une utilisation plus *réfléchie* de leurs **outils**.

- Particulièrement vrai lorsque ces outils cachent une grande partie de leur fonctionnement interne

On ne rentrera pas dans les détails des points suivants :



On ne rentrera pas dans les détails des points suivants :

- le **chiffrement** en lui-même, notamment les différents algorithmes pouvant être utilisés
  - On ne cherche pas à développer la *maîtrise* du chiffrement, simplement son utilisation *réfléchie*

On ne rentrera pas dans les détails des points suivants :

- le **chiffrement** en lui-même, notamment les différents algorithmes pouvant être utilisés
  - On ne cherche pas à développer la *maîtrise* du chiffrement, simplement son utilisation *réfléchie*
- les **vulnérabilités** de nos messageries ou des protocoles qu'elles utilisent
  - métadonnées dans les en-têtes d'e-mail
  - adresses IP loggées lors des communications via SMTP
  - etc.

- On a pas besoin d'être un·e **expert·e** en informatique pour pouvoir chiffrer ses e-mails

# Notes sur les outils utilisés pendant cette présentation

- On a pas besoin d'être un·e **expert·e** en informatique pour pouvoir chiffrer ses e-mails
- Une partie de la présentation se fera dans un **terminal de commande**

- On a pas besoin d'être un-e **expert·e** en informatique pour pouvoir chiffrer ses e-mails
- Une partie de la présentation se fera dans un **terminal de commande**
  - Il s'agit simplement d'une différente **grammaire** pour communiquer avec les programmes
  - Au lieu de pointer avec la souris, on *parle* avec le programme
  - Les démonstrations seront **commentées**; aucune connaissance n'est requise

# Pourquoi chiffrer ses e-mails?

# Pourquoi chiffrer ses e-mails?

- **Chiffrer** ses e-mails permet de s'assurer qu'**aucune autre personne** que le **destinataire·rice** ne puisse lire leurs contenus
  - On **sécurise** la communication

# Pourquoi chiffrer ses e-mails ?

- **Chiffrer** ses e-mails permet de s'assurer qu'**aucune autre personne** que le **destinataire·rice** ne puisse lire leurs contenus
  - On **sécurise** la communication
- En parallèle du chiffrement, **signer** ses e-mails permet de nous **identifier** comme étant l'auteur·rice réel·le du message
  - On **authentifie** la communication



# Chiffrement symétrique

- 1 Introduction
- 2 Chiffrement symétrique
  - Vocabulaire
  - Les bases
  - Deux exemples
  - Cas pratique
  - Les limites du chiffrement symétrique
- 3 Chiffrement asymétrique
- 4 GPG : Explication

Quelques termes :

Quelques termes :

- chiffrer
- déchiffrer

Quelques termes :

- chiffrer

- déchiffrer

- texte *en clair*  $\xrightarrow{\text{chiffage}}$

Quelques termes :

- chiffrer

- déchiffrer

- texte *en clair*  $\xrightarrow{\text{chiffage}}$  texte *chiffré*

Quelques termes :

- chiffrer

- déchiffrer

- texte *en clair*  $\xrightarrow{\text{chiffage}}$  texte *chiffré*

Français	Équivalent anglais	Anglicisme
chiffrer	<i>to encrypt / to cipher</i>	* crypter
déchiffrer	<i>to decrypt / to decipher</i>	* décripter
texte clair	<i>plaintext</i>	
texte chiffré	<i>ciphertext</i>	

# Les bases du chiffrement symétrique

- Une clé pour le **chiffage**



# Les bases du chiffrement symétrique

- Une clé pour le **chiffage**
- La **même** clé pour le **déchiffage**

# Les bases du chiffrement symétrique

- Une clé pour le **chiffage**
- La **même** clé pour le **déchiffage**

Une seule clé, d'où la notion de **symétrie**

# Les bases du chiffrement symétrique

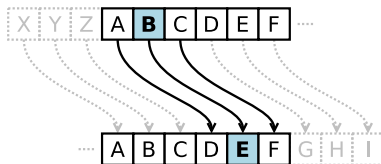
- Une clé pour le **chiffage**
- La **même** clé pour le **déchiffage**

Une seule clé, d'où la notion de **symétrie**

## Analogie visuelle : un coffre

- On le **verrouille** avec une clé
- On le **déverrouille** avec la **même** clé

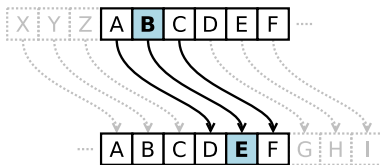
# Exemples de chiffrements symétriques



*Caesar cipher with a shift of 3 par Matt\_Crypto / Domaine Public*

**FIGURE** – Chiffrement par décalage, ou chiffre de César

# Exemples de chiffrements symétriques



*Caesar cipher with a shift of 3 par Matt\_Crypto / Domaine Public*

**FIGURE** – Chiffrement par décalage, ou chiffre de César



*Enigma par Alessandro Nassiri / CC BY-SA-4.0*

**FIGURE** – Les *Enigma machines*



# Exemple pratique

Communication par chiffrement symétrique

Sophie et Marc veulent s'échanger des **lettres secrètes**

# Exemple pratique

Communication par chiffrement symétrique

Sophie et Marc veulent s'échanger des **lettres secrètes**

- Pour s'assurer qu'aucune autre personne ne lise leurs messages, Sophie et Marc s'accorde sur le fait d'utiliser le **chiffre de César** pour chiffrer leur communication



# Exemple pratique

## Communication par chiffrement symétrique

Sophie et Marc veulent s'échanger des **lettres secrètes**

- Pour s'assurer qu'aucune autre personne ne lise leurs messages, Sophie et Marc s'accorde sur le fait d'utiliser le **chiffre de César** pour chiffrer leur communication
- Lorsque l'un-e des participant-e-s veut **envoyer** une lettre secrète à l'autre, la personne doit effectuer le **chiffrement** du **texte clair**

# Exemple pratique

## Communication par chiffrement symétrique

Sophie et Marc veulent s'échanger des **lettres secrètes**

- Pour s'assurer qu'aucune autre personne ne lise leurs messages, Sophie et Marc s'accorde sur le fait d'utiliser le **chiffre de César** pour chiffrer leur communication
- Lorsque l'un-e des participant-e-s veut **envoyer** une lettre secrète à l'autre, la personne doit effectuer le **chiffrement** du **texte clair**

*Mes secrets les plus sombres*  $\xrightarrow[\text{-3}]{\text{chiffre de César}}$  Jbp pbzobqp ibp mirp pljyobp

# Exemple pratique

## Communication par chiffrement symétrique

Sophie et Marc veulent s'échanger des **lettres secrètes**

- Pour s'assurer qu'aucune autre personne ne lise leurs messages, Sophie et Marc s'accorde sur le fait d'utiliser le **chiffre de César** pour chiffrer leur communication
- Lorsque l'un-e des participant-e-s veut **envoyer** une lettre secrète à l'autre, la personne doit effectuer le **chiffrement** du **texte clair**

*Mes secrets les plus sombres*  $\xrightarrow[\text{-3}]{\text{chiffre de César}}$  Jbp pbzobqp ibp mirp pljyobp

- Lorsque l'un-e des participant-e-s veut **lire** une lettre secrète de l'autre, la personne doit effectuer le **déchiffrement** du **texte chiffré**

# Exemple pratique

## Communication par chiffrement symétrique

Sophie et Marc veulent s'échanger des **lettres secrètes**

- Pour s'assurer qu'aucune autre personne ne lise leurs messages, Sophie et Marc s'accorde sur le fait d'utiliser le **chiffre de César** pour chiffrer leur communication
- Lorsque l'un-e des participant-e-s veut **envoyer** une lettre secrète à l'autre, la personne doit effectuer le **chiffrement** du **texte clair**

*Mes secrets les plus sombres*  $\xrightarrow[\text{-3}]{\text{chiffre de César}}$  Jbp pbzobqp ibp mirp pljyobp

- Lorsque l'un-e des participant-e-s veut **lire** une lettre secrète de l'autre, la personne doit effectuer le **déchiffrement** du **texte chiffré**

Jbp pbzobqp ibp mirp pljyobp  $\xrightarrow[\text{+3}]{\text{chiffre de César}}$  *Mes secrets les plus sombres*

# Un grand problème

# Un grand problème

Dans notre exemple, le problème à résoudre est **très facile**

Dans notre exemple, le problème à résoudre est **très facile**

- Les *fréquences d'apparition* des lettres sont conservées

Dans notre exemple, le problème à résoudre est **très facile**

- Les *fréquences d'apparition* des lettres sont conservées
- On peut facilement utiliser la *force brute* et essayer toutes les *permutations* possibles (26) jusqu'à obtenir un texte qui fasse sens



Dans notre exemple, le problème à résoudre est **très facile**

- Les *fréquences d'apparition* des lettres sont conservées
- On peut facilement utiliser la *force brute* et essayer toutes les *permutations* possibles (26) jusqu'à obtenir un texte qui fasse sens

## Notion de sécurité

Dans notre exemple, le problème à résoudre est **très facile**

- Les *fréquences d'apparition* des lettres sont conservées
- On peut facilement utiliser la *force brute* et essayer toutes les *permutations* possibles (26) jusqu'à obtenir un texte qui fasse sens

## Notion de sécurité

- La **sécurité** d'une communication dépend de la **difficulté** du **problème** qu'elle utilise pour chiffrer ses messages

Dans notre exemple, le problème à résoudre est **très facile**

- Les *fréquences d'apparition* des lettres sont conservées
- On peut facilement utiliser la *force brute* et essayer toutes les *permutations* possibles (26) jusqu'à obtenir un texte qui fasse sens

## Notion de sécurité

- La **sécurité** d'une communication dépend de la **difficulté** du **problème** qu'elle utilise pour chiffrer ses messages
- Plus un problème est **facile** à résoudre, plus il sera **facile** pour un-e ennemi-e de **cracker** notre communication

Dans notre exemple, le problème à résoudre est **très facile**

- Les *fréquences d'apparition* des lettres sont conservées
- On peut facilement utiliser la *force brute* et essayer toutes les *permutations* possibles (26) jusqu'à obtenir un texte qui fasse sens

## Notion de sécurité

- La **sécurité** d'une communication dépend de la **difficulté** du **problème** qu'elle utilise pour chiffrer ses messages
- Plus un problème est **facile** à résoudre, plus il sera **facile** pour un-e ennemi-e de **cracker** notre communication

Il nous faut donc trouver des problèmes plus **difficiles** à résoudre

- 1 Introduction
- 2 Chiffrement symétrique
- 3 Chiffrement asymétrique**
  - Les bases
  - Analogie
  - Retour au réel
- 4 GPG : Explication

# Les bases du chiffrement asymétrique

- Une clé pour le **chiffage**

# Les bases du chiffrement asymétrique

- Une clé pour le **chiffage**
- Une **autre** clé pour le **déchiffage**



# Les bases du chiffrement asymétrique

- Une clé pour le **chiffage**
- Une **autre** clé pour le **déchiffage**

Deux clés différentes, d'où la notion d'**asymétrie**

# Les bases du chiffrement asymétrique

- Une clé pour le **chiffage**
- Une **autre** clé pour le **déchiffage**

Deux clés différentes, d'où la notion d'**asymétrie**

Analogie visuelle : un coffre *magique*

- On le **verrouille** avec une clé
- On le **déverrouille** avec une **autre** clé



- Sophie a la clé pour [fermer](#) le coffre magique

- Sophie a la clé pour fermer le coffre magique
- Marc a la clé pour ouvrir le coffre magique

- Sophie a la clé pour fermer le coffre magique
- Marc a la clé pour ouvrir le coffre magique

Quel est l'intérêt ?

- Sophie a la clé pour fermer le coffre magique
- Marc a la clé pour ouvrir le coffre magique

Quel est l'intérêt ?

- Si les clés sont en possession de **deux personnes différentes**, le coffre magique crée un **canal de communication sécurisé** entre celles-ci

- Sophie a la clé pour **fermer** le coffre magique
- Marc a la clé pour **ouvrir** le coffre magique

Quel est l'intérêt ?

- Si les clés sont en possession de **deux personnes différentes**, le coffre magique crée un **canal de communication sécurisé** entre celles-ci

Question



- Sophie a la clé pour **fermer** le coffre magique
- Marc a la clé pour **ouvrir** le coffre magique

Quel est l'intérêt ?

- Si les clés sont en possession de **deux personnes différentes**, le coffre magique crée un **canal de communication sécurisé** entre celles-ci

## Question

- Marc trouve le coffre magique **verrouillé**

- Sophie a la clé pour **fermer** le coffre magique
- Marc a la clé pour **ouvrir** le coffre magique

Quel est l'intérêt ?

- Si les clés sont en possession de **deux personnes différentes**, le coffre magique crée un **canal de communication sécurisé** entre celles-ci

## Question

- Marc trouve le coffre magique **verrouillé**
- Après l'avoir **déverrouillé** et ouvert, il y trouve un **paquet cadeau**

- Sophie a la clé pour **fermer** le coffre magique
- Marc a la clé pour **ouvrir** le coffre magique

Quel est l'intérêt ?

- Si les clés sont en possession de **deux personnes différentes**, le coffre magique crée un **canal de communication sécurisé** entre celles-ci

## Question

- Marc trouve le coffre magique **verrouillé**
- Après l'avoir **déverrouillé** et ouvert, il y trouve un **paquet cadeau**

Peut-on conclure que c'est Sophie qui l'y a mis ?

- Sophie a la clé pour **fermer** le coffre magique
- Marc a la clé pour **ouvrir** le coffre magique

Quel est l'intérêt ?

- Si les clés sont en possession de **deux personnes différentes**, le coffre magique crée un **canal de communication sécurisé** entre celles-ci

## Question

- Marc trouve le coffre magique **verrouillé**
- Après l'avoir **déverrouillé** et ouvert, il y trouve un **paquet cadeau**

Peut-on conclure que c'est Sophie qui l'y a mis? **NON!**

- Sophie a la clé pour **fermer** le coffre magique
- Marc a la clé pour **ouvrir** le coffre magique

Quel est l'intérêt ?

- Si les clés sont en possession de **deux personnes différentes**, le coffre magique crée un **canal de communication sécurisé** entre celles-ci

## Question

- Marc trouve le coffre magique **verrouillé**
- Après l'avoir **déverrouillé** et ouvert, il y trouve un **paquet cadeau**

Peut-on conclure que c'est Sophie qui l'y a mis? **NON!**

- On peut juste dire que la clé de Sophie a été utilisée

- Sophie a la clé pour **fermer** le coffre magique
- Marc a la clé pour **ouvrir** le coffre magique

Quel est l'intérêt ?

- Si les clés sont en possession de **deux personnes différentes**, le coffre magique crée un **canal de communication sécurisé** entre celles-ci

## Question

- Marc trouve le coffre magique **verrouillé**
- Après l'avoir **déverrouillé** et ouvert, il y trouve un **paquet cadeau**

Peut-on conclure que c'est Sophie qui l'y a mis ? **NON !**

- On peut juste dire que la clé de Sophie a été utilisée
- On n'a aucun moyen de vérifier s'il s'agit vraiment d'elle

- Sophie a la clé pour **fermer** le coffre magique
- Marc a la clé pour **ouvrir** le coffre magique

Quel est l'intérêt ?

- Si les clés sont en possession de **deux personnes différentes**, le coffre magique crée un **canal de communication sécurisé** entre celles-ci

## Question

- Marc trouve le coffre magique **verrouillé**
- Après l'avoir **déverrouillé** et ouvert, il y trouve un **paquet cadeau**

Peut-on conclure que c'est Sophie qui l'y a mis ? **NON !**

- On peut juste dire que la clé de Sophie a été utilisée
- On n'a aucun moyen de vérifier s'il s'agit vraiment d'elle
  - Rien ne permet d'**authentifier** la communication

Solution



## Solution

- En sortant de la boutique du magicien, Sophie et Marc s'accordent sur un **mot de passe**
- À chaque fois que Sophie veut déposer quelque chose dans le coffre magique, elle devra aussi inclure ce **mot de passe** écrit sur une feuille

## Solution

- En sortant de la boutique du magicien, Sophie et Marc s'accordent sur un **mot de passe**
- À chaque fois que Sophie veut déposer quelque chose dans le coffre magique, elle devra aussi inclure ce **mot de passe** écrit sur une feuille

C'est la base du **MFA** (*Multi-Factor Authentication*)

- Combinaison entre quelque chose que l'on **sait** (le **mot de passe**) et quelque chose que l'on **a** (la **clé**)

# Deux conclusions

1. Le coffre magique permet une **communication sécurisée** entre les détenteur·rice·s des clés

# Deux conclusions

1. Le coffre magique permet une **communication sécurisée** entre les détenteur·rice·s des clés
2. Le mot de passe permet d'**authentifier** l'expéditeur·rice

# Deux problèmes

# Deux problèmes

1. Sophie ne peut pas rouvrir le coffre une fois qu'il est fermé

Solution?

# Deux problèmes

1. Sophie ne peut pas rouvrir le coffre une fois qu'il est fermé

## Solution?

- Pas un **problème** mais un **avantage**



# Deux problèmes

1. Sophie ne peut pas rouvrir le coffre une fois qu'il est fermé

## Solution?

- Pas un **problème** mais un **avantage**
- Après la fermeture du coffre magique, la **surface d'attaque** est limitée à la clé de Marc

# Deux problèmes

1. Sophie ne peut pas rouvrir le coffre une fois qu'il est fermé

## Solution?

- Pas un **problème** mais un **avantage**
- Après la fermeture du coffre magique, la **surface d'attaque** est limitée à la clé de Marc
- Si un-e **ennemi-e** intercepte la clé de Sophie après la fermeture du coffre, il ne pourra pas modifier le contenu du coffre magique avant que Marc ne l'ouvre

# Deux problèmes

1. Sophie ne peut pas rouvrir le coffre une fois qu'il est fermé

## Solution?

- Pas un **problème** mais un **avantage**
- Après la fermeture du coffre magique, la **surface d'attaque** est limitée à la clé de Marc
- Si un-e **ennemi-e** intercepte la clé de Sophie après la fermeture du coffre, il ne pourra pas modifier le contenu du coffre magique avant que Marc ne l'ouvre

2. Sophie peut communiquer avec Marc, mais pas l'**inverse**

- La communication est *unilatérale*

## Solution?

# Deux problèmes

1. Sophie ne peut pas rouvrir le coffre une fois qu'il est fermé

## Solution?

- Pas un **problème** mais un **avantage**
- Après la fermeture du coffre magique, la **surface d'attaque** est limitée à la clé de Marc
- Si un-e **ennemi-e** intercepte la clé de Sophie après la fermeture du coffre, il ne pourra pas modifier le contenu du coffre magique avant que Marc ne l'ouvre

2. Sophie peut communiquer avec Marc, mais pas l'**inverse**

- La communication est *unilatérale*

## Solution?

Sophie et Marc doivent acheter un **autre** coffre magique pour assurer la communication dans le **sens inverse**

# Relier l'analogie au réel

Du coffre magique à la boîte mail

Quelques propriétés d'une boîte aux lettres :

# Relier l'analogie au réel

Du coffre magique à la boîte mail

Quelques propriétés d'une boîte aux lettres :

1. C'est un espace physique qui est clairement **identifié** comme nous appartenant
  - Il possède des **marqueurs** de notre **identité** (adresse, nom, etc.)

# Relier l'analogie au réel

Du coffre magique à la boîte mail

Quelques propriétés d'une boîte aux lettres :

1. C'est un espace physique qui est clairement **identifié** comme nous appartenant
  - Il possède des **marqueurs** de notre **identité** (adresse, nom, etc.)
2. C'est un espace **clos** dont nous sommes les **seul·e·s** à pouvoir consulter le contenu
  - Nous sommes les **seul·e·s** à avoir la **clé** de notre boîte aux lettres

# Relier l'analogie au réel

Du coffre magique à la boîte mail

Quelques propriétés d'une boîte aux lettres :

1. C'est un espace physique qui est clairement **identifié** comme nous appartenant
  - Il possède des **marqueurs** de notre **identité** (adresse, nom, etc.)
2. C'est un espace **clos** dont nous sommes les **seul·e·s** à pouvoir consulter le contenu
  - Nous sommes les **seul·e·s** à avoir la **clé** de notre boîte aux lettres
3. N'importe quelle personne ayant notre adresse peut y déposer des messages



# Relier l'analogie au réel

Du coffre magique à la boîte mail

Quelques propriétés d'une boîte aux lettres :

1. C'est un espace physique qui est clairement **identifié** comme nous appartenant
  - Il possède des **marqueurs** de notre **identité** (adresse, nom, etc.)
2. C'est un espace **clos** dont nous sommes les **seul·e·s** à pouvoir consulter le contenu
  - Nous sommes les **seul·e·s** à avoir la **clé** de notre boîte aux lettres
3. N'importe quelle personne ayant notre adresse peut y déposer des messages

## Deux remarques

# Relier l'analogie au réel

Du coffre magique à la boîte mail

Quelques propriétés d'une boîte aux lettres :

1. C'est un espace physique qui est clairement **identifié** comme nous appartenant
  - Il possède des **marqueurs** de notre **identité** (adresse, nom, etc.)
2. C'est un espace **clos** dont nous sommes les **seul·e·s** à pouvoir consulter le contenu
  - Nous sommes les **seul·e·s** à avoir la **clé** de notre boîte aux lettres
3. N'importe quelle personne ayant notre adresse peut y déposer des messages

## Deux remarques

- Une boîte mail fonctionne selon les **mêmes** paramètres qu'une **boîte aux lettres**
  - Au lieu d'un espace **physique**, on parle d'un espace **virtuel**

# Relier l'analogie au réel

Du coffre magique à la boîte mail

Quelques propriétés d'une boîte aux lettres :

1. C'est un espace physique qui est clairement **identifié** comme nous appartenant
  - Il possède des **marqueurs** de notre **identité** (adresse, nom, etc.)
2. C'est un espace **clos** dont nous sommes les **seul·e·s** à pouvoir consulter le contenu
  - Nous sommes les **seul·e·s** à avoir la **clé** de notre boîte aux lettres
3. N'importe quelle personne ayant notre adresse peut y déposer des messages

## Deux remarques

- Une boîte mail fonctionne selon les **mêmes** paramètres qu'une **boîte aux lettres**
  - Au lieu d'un espace **physique**, on parle d'un espace **virtuel**
- Pas besoin de *magie* dans le monde virtuel, juste d'**algorithmes**

- 1 Introduction
- 2 Chiffrement symétrique
- 3 Chiffrement asymétrique
- 4 GPG : Explication**
  - Clé privée & clé publique
  - Explication de l'algorithme

Sophie et Marc ont chacun une *paire* de **clés virtuelles**

Chaque paire comporte :

- une **clé privée**
- une **clé publique**

Quelques propriétés d'une *bonne* clé **physique** :

Quelques propriétés d'une *bonne* clé **physique** :

1. Elle est **reliée** à un objet (porte, coffre, etc.)

Quelques propriétés d'une *bonne* clé **physique** :

1. Elle est **reliée** à un objet (porte, coffre, etc.)
2. Sa *forme* ne nous permet pas de **deviner** l'objet qu'elle **protège**



Quelques propriétés d'une *bonne* clé **physique** :

1. Elle est **reliée** à un objet (porte, coffre, etc.)
2. Sa *forme* ne nous permet pas de **deviner** l'objet qu'elle **protège**
3. Sa *forme* est difficile à **deviner** ou à **copier** pour les *humains*
  - Un certain nombre de dents
  - Une certaine hauteur pour chaque dent
  - etc.

Quelques propriétés d'une *bonne* clé **physique** :

1. Elle est **reliée** à un objet (porte, coffre, etc.)
2. Sa *forme* ne nous permet pas de **deviner** l'objet qu'elle **protège**
3. Sa *forme* est difficile à **deviner** ou à **copier** pour les *humains*
  - Un certain nombre de dents
  - Une certaine hauteur pour chaque dent
  - etc.
4. Si elle est **perdue** ou **volée**, l'**accès** à l'objet qu'elle protège et sa **sécurité** sont remis·e·s en question

Quelques propriétés d'une *bonne* clé **virtuelle** :

Quelques propriétés d'une *bonne* clé **virtuelle** :

1. Elle est **reliée** à un objet (e-mail, site, etc.)

Quelques propriétés d'une *bonne* clé **virtuelle** :

1. Elle est **reliée** à un objet (e-mail, site, etc.)
2. Son *contenu* ne nous permet pas de **deviner** le compte qu'elle **protège**

Quelques propriétés d'une *bonne* clé **virtuelle** :

1. Elle est **reliée** à un objet (e-mail, site, etc.)
2. Son *contenu* ne nous permet pas de **deviner** le compte qu'elle **protège**
3. Son *contenu* est difficile à **deviner** ou à **copier** pour les *humains*
  - Un grand nombre de *caractères alphanumériques et spéciaux* générés **aléatoirement** (au moins 2048)

Quelques propriétés d'une *bonne* clé **virtuelle** :

1. Elle est **reliée** à un objet (e-mail, site, etc.)
2. Son *contenu* ne nous permet pas de **deviner** le compte qu'elle **protège**
3. Son *contenu* est difficile à **deviner** ou à **copier** pour les *humains*
  - Un grand nombre de *caractères alphanumériques et spéciaux* générés **aléatoirement** (au moins 2048)
4. Si elle **perdue** ou **volée**, l'**accès** au contenu qu'elle protège et sa **sécurité** sont remis·e·s en question

# Exemple de clé virtuelle

```
1 -----BEGIN PGP PUBLIC KEY BLOCK-----
2
3 mQINBFA1+ugBEADuoZPjHs6+ME9Wm3c94IqqUhwEEFJ3xz1sYJus4V8GMW9TEy1L
4 iQGwx5p1+6yOi+D/tvW3q9jmerdI+EWvQeUvrwx6r4razTZTe1+48u0jhko85SM
5 xDzEF9wf2gGEt0abZamUu86kfMcmPFMVoGLoLI/7feAscP4iGMK9ZlX+C/1wzq20
6 gujHxDMv7QoYvII7wJrPm4NZHM2MUxLwxhjifb8JZPE0WGyUJ5+FsPEreh0MgC0
7 R53Eo6wIzTU4cBB/dyabI/2/jn2Ya0svoC9B1M8N9mG/bxSqTETiQrgcA1bk0zHj
8 qiy4fXImi+Gkacbwrdad9QkRVCHSXu/pN6iqZiUvXvfmA0bjRYsoY3JPfjGCTyF
9 58ZELfHnGx6MQtF6Dj0wX7qMBY0jh000n0znmwVp1MLm5Augs6hAvX8VF99KQVtc
10 mEUUnb+Gxc7Y2MBFjWvTpiVwcXAZt8z13gE6UP1s+X5JKdDqXLqCLR2cq82+EBtS0
11 8U7j00acGGCU3+2/fL8T4KGv1XnUN50nqCb21m076dEsHi2k8016/XPocaLSxzQF
12 ZVRcLsmvD1hct367+mxrrvANmn17YyljGzjs0fMv5duxnpVpbLFRYz0g4BC2wMb
13 H1KtLfc+b1XkVmvICax+OTE8bP+Yo01qW2gkB6wUrjAyeBuuxwJXF59XmwARAQAB
14 tDZUYWlscyBzeXN0Zl0gYWRtaW5pc3RyYXRvcnMgPHRhaWxzLXN5c2FkbWluc0Bi
15 b3VtLm9yZz6JAj4EEwECACgFA1A1+ugCGwMFCQPCZwAGCwkIBwMCBhUIAgkKCwQW
16 AgMBAh4BAheAAA0JEHD08DEWU19DjNEP/RnRhbw30AsMEXptsZmUGo9jUAoeWiug
17 Yr5uZ8aiQGTynTh08wzHKR0imPvZ7Ctaszo1q20/VAcdocZdCRD5bmdXgsHfPeK0
18 sKcBGAe+pa0tiF0up1rLxcB1MPz7bUCvTn5AMin3lhFzLTdq5ei6AkOitaG0Kn5v
19 /E066gsGVJ+edxrMbi+vIOa+cf3bIolgaPERGUQJKahZUKstws0xiXAucZ1QePdQ
20 Yj1zt6XhLe+xvHPN04XWucI1hXm/8RHZcxTbhkt1+kXpIALBjewWraHTtgP0mmXG
21 MDV00bE3qpiNw2451mRu3ypJGotjq1wo8fPMAgcus/3wEn1VUrsYgTR2gUzXVc1
22 ...
```



# Clé virtuelle vs. mot de passe

Quelles sont les différences entre une *clé virtuelle* et un *mot de passe*?

# Clé virtuelle vs. mot de passe

Quelles sont les différences entre une *clé virtuelle* et un *mot de passe*?

- Une *clé virtuelle* est beaucoup plus **robuste** que les *mots de passe* traditionnels
  - $\geq 2048$  caractères pour les *clés virtuelles* contre  $< 30$  pour les *mots de passe* traditionnels

Quelles sont les différences entre une *clé virtuelle* et un *mot de passe*?

- Une *clé virtuelle* est beaucoup plus **robuste** que les *mots de passe* traditionnels
  - $\geq 2048$  caractères pour les *clés virtuelles* contre  $< 30$  pour les *mots de passe* traditionnels
- Une *clé virtuelle* n'a pas pour but d'être **manipulée** par son utilisateur
  - Trop longue pour être **mémorisée**
  - Trop longue pour être **entrée** à chaque utilisation

# Clé virtuelle vs. mot de passe

Quelles sont les différences entre une *clé virtuelle* et un *mot de passe*?

- Une *clé virtuelle* est beaucoup plus **robuste** que les *mots de passe* traditionnels
  - $\geq 2048$  caractères pour les *clés virtuelles* contre  $< 30$  pour les *mots de passe* traditionnels
- Une *clé virtuelle* n'a pas pour but d'être **manipulée** par son utilisateur
  - Trop longue pour être **mémorisée**
  - Trop longue pour être **entrée** à chaque utilisation
- Les deux ne sont pas exclusif·ve·s
  - Une *clé virtuelle* est souvent elle-même protégée par un *mot de passe*
  - Combine le côté **pratique** d'un *mot de passe* avec la **robustesse** d'une *clé virtuelle*

# Lien avec l'analogie du coffre magique

On désigne le coffre que Marc peut ouvrir comme étant « le coffre de Marc »

# Lien avec l'analogie du coffre magique

On désigne le coffre que Marc peut ouvrir comme étant « le coffre de Marc »

- La **clé privée** de Marc est celle qu'il utilise pour **ouvrir** son coffre

# Lien avec l'analogie du coffre magique

On désigne le coffre que Marc peut ouvrir comme étant « le coffre de Marc »

- La **clé privée** de Marc est celle qu'il utilise pour **ouvrir** son coffre
- La **clé publique** de Marc est celle qu'il donne à Sophie pour pouvoir **fermer** son coffre

# Lien avec l'analogie du coffre magique

On désigne le coffre que Marc peut ouvrir comme étant « le coffre de Marc »

- La **clé privée** de Marc est celle qu'il utilise pour **ouvrir** son coffre
- La **clé publique** de Marc est celle qu'il donne à Sophie pour pouvoir **fermer** son coffre

Pourquoi parle-t-on de « **clé publique** » ?



# Pourquoi « publique » ?

# Pourquoi « publique » ?

- On parle de clé « publique » parce qu'elle est destinée à être **partagée** avec les personnes avec qui on souhaite communiquer (le « public »)

# Pourquoi « publique » ?

- On parle de **clé « publique »** parce qu'elle est destinée à être **partagée** avec les personnes avec qui on souhaite communiquer (le « public »)
- Le fait que la clé soit qualifiée de « **public** » ne veut pas dire que les **communications** se faisant avec elles le sont
  - Même si la **clé publique** est partagée avec des **ennemi·e·s**, cela ne leur apporte **aucune information utile** pour *cracker* le chiffrement

# Pourquoi « publique » ?

- On parle de **clé « publique »** parce qu'elle est destinée à être **partagée** avec les personnes avec qui on souhaite communiquer (le « public »)
- Le fait que la clé soit qualifiée de « **public** » ne veut pas dire que les **communications** se faisant avec elles le sont
  - Même si la **clé publique** est partagée avec des **ennemi·e·s**, cela ne leur apporte **aucune information utile** pour *cracker* le chiffrement
- Notre **clé publique** n'est qu'un autre **marqueur** de notre **identité**
  - Il existe des annuaires de **clés publiques**
  - Notre **clé publique** est identifiée dans les annuaires par notre **nom** et notre **adresse e-mail**
  - On peut trouver notre **clé publique** dans ces annuaires en cherchant l'un·e des deux

# Pourquoi « publique » ?

- On parle de **clé « publique »** parce qu'elle est destinée à être **partagée** avec les personnes avec qui on souhaite communiquer (le « public »)
- Le fait que la clé soit qualifiée de « **public** » ne veut pas dire que les **communications** se faisant avec elles le sont
  - Même si la **clé publique** est partagée avec des **ennemi·e·s**, cela ne leur apporte **aucune information utile** pour *cracker* le chiffrement
- Notre **clé publique** n'est qu'un autre **marqueur** de notre **identité**
  - Il existe des annuaires de **clés publiques**
  - Notre **clé publique** est identifiée dans les annuaires par notre **nom** et notre **adresse e-mail**
  - On peut trouver notre **clé publique** dans ces annuaires en cherchant l'un·e des deux

Un problème avec les noms

# Pourquoi « publique » ?

- On parle de **clé « publique »** parce qu'elle est destinée à être **partagée** avec les personnes avec qui on souhaite communiquer (le « public »)
- Le fait que la clé soit qualifiée de « **public** » ne veut pas dire que les **communications** se faisant avec elles le sont
  - Même si la **clé publique** est partagée avec des **ennemi·e·s**, cela ne leur apporte **aucune information utile** pour *cracker* le chiffrement
- Notre **clé publique** n'est qu'un autre **marqueur** de notre **identité**
  - Il existe des annuaires de **clés publiques**
  - Notre **clé publique** est identifiée dans les annuaires par notre **nom** et notre **adresse e-mail**
  - On peut trouver notre **clé publique** dans ces annuaires en cherchant l'un-e des deux

## Un problème avec les noms

Les **noms** sont rarement **uniques**, à l'opposé des **adresses e-mail**

Si l'*anonymat* ou le *pseudonymat* est désirable, on peut jouer sur certains paramètres :

Si l'*anonymat* ou le *pseudonymat* est désirable, on peut jouer sur certains paramètres :

- Utiliser un pseudonyme **et** une **autre** adresse



Si l'*anonymat* ou le *pseudonymat* est désirable, on peut jouer sur certains paramètres :

- Utiliser un pseudonyme **et** une **autre** adresse
- Ne pas être référencé dans les annuaires
  - Le référencement n'est pas automatique
  - Ajoute du travail pour un gain marginal

# Lien entre clé privée et clé publique

La *magie* du coffre

Les deux clés sont générées en même temps par un même **algorithme**

# Lien entre clé privée et clé publique

La *magie* du coffre

Les deux clés sont générées en même temps par un même **algorithme**  
Comment est-ce que ça marche ?

# Lien entre clé privée et clé publique

La *magie* du coffre

Les deux clés sont générées en même temps par un même **algorithme**  
Comment est-ce que ça marche ?

Principe de la cryptographie asymétrique

# Lien entre clé privée et clé publique

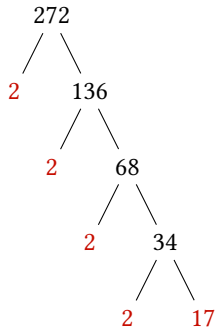
La *magie* du coffre

Les deux clés sont générées en même temps par un même **algorithme**  
Comment est-ce que ça marche ?

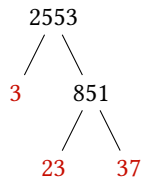
## Principe de la cryptographie asymétrique

La **cryptographie asymétrique** est basée sur la création de **problèmes mathématiques difficiles** à résoudre dans un *sens* mais **faciles** à résoudre dans un autre

# Exemple : Décomposition en nombres premiers

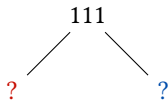


Résultat : {2, 2, 2, 2, 17}

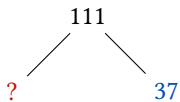


Résultat : {3, 23, 37}

# Une difficulté croissante

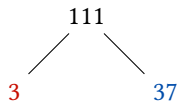


# Une difficulté croissante



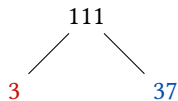


# Une difficulté croissante

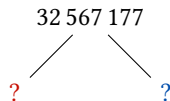


Résultat : {3, 37}

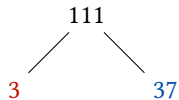
# Une difficulté croissante



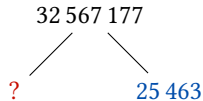
Résultat : {3, 37}



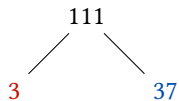
# Une difficulté croissante



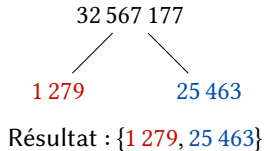
Résultat : {3, 37}



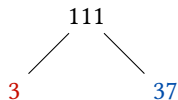
# Une difficulté croissante



Résultat : {3, 37}



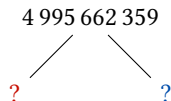
# Une difficulté croissante



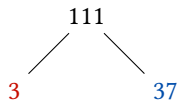
Résultat : {3, 37}



Résultat : {1 279, 25 463}



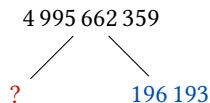
# Une difficulté croissante



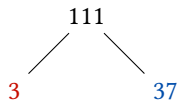
Résultat : {3, 37}



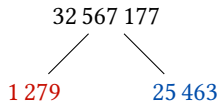
Résultat : {1 279, 25 463}



# Une difficulté croissante



Résultat : {3, 37}



Résultat : {1 279, 25 463}



Résultat : {25 463, 196 193}

# Observations



1. Multiplier deux nombres pour en obtenir un troisième est **facile**

1. Multiplier deux nombres pour en obtenir un troisième est **facile**
2. Trouver ces deux nombres en n'ayant que le troisième est **difficile**
  - C'est le problème que doivent résoudre nos *ennemi·e·s*

1. Multiplier deux nombres pour en obtenir un troisième est **facile**
2. Trouver ces deux nombres en n'ayant que le troisième est **difficile**
  - C'est le problème que doivent résoudre nos *ennemi·e·s*
3. Trouver l'un des deux nombres lorsqu'on a l'autre et le troisième est **facile** (on **divise**)
  - C'est le problème que doit résoudre le *destinataire·rice*

L'algorithme assure que chaque problème généré par la **clé public** est **difficile** à résoudre pour **tout le monde** sauf pour le **destinataire**.

L'algorithme assure que chaque problème généré par la **clé public** est **difficile** à résoudre pour **tout le monde** sauf pour le **destinataire**.

- La **clé privée** dispose de **plus d'informations** pour chaque problème
  - Par exemple, lors d'une décomposition en facteurs premiers, déjà avoir l'un des facteurs

# Démonstration

## Notes

- La démonstration s'est faite dans un *terminal de commande* et avait pour but de **relier** les différents concepts abordés lors de la présentation
- Elle a aussi exploré le lien entre *texte simple* (*plaintext*<sup>a</sup> en anglais) et *e-mail* en précisant notamment qu'un e-mail n'est que du texte accompagné d'un *en-tête* pour contenir des informations sur l'expéditeur·rice et le·a destinataire·rice

---

a. *Plaintext* désigne à la fois un texte *non-chiffré* et un texte *sans formatage*. Par exemple, les fichiers avec une extension `.txt` sont souvent des fichiers en *plaintext*

Fin de la présentation



- 1 Pour aller plus loin
- 2 Références
- 3 Informations supplémentaires

## Aspects généraux de sécurité :

- **Mathieu Goessens**, *Quelques notions de sécurité*, 2018, URL : <http://mathieu.goessens.fr/formation/formation.pdf> (visité le 30/01/2019)
- **La Fondation « Frontière Électronique »**, *Surveillance Self-Defence*, s. d., URL : <https://ssd.eff.org/fr> (visité le 30/01/2019)

## Guides avancés :

- **Reporters Sans Frontières**, *Guide Pratique de Sécurité des Journalistes*, 2017, URL : [https://rsf.org/sites/default/files/guide\\_fr\\_2017\\_1.pdf](https://rsf.org/sites/default/files/guide_fr_2017_1.pdf) (visité le 30/01/2019)
- **Les boumeur·euse·s**, *Guide d'autodéfense numérique*, 10 sept. 2017, URL : <https://guide.boum.org/> (visité le 30/01/2019)

## Ressources en anglais :

- **GNUPG**, *GNUPG Frequently Asked Questions*, s. d., URL : <https://www.gnupg.org/faq/gnupg-faq.html> (visité le 30/01/2019)
- **GNUPG**, *The GNU Privacy Guard Manual*, déc. 2018, URL : <https://www.gnupg.org/documentation/manuals/gnupg/> (visité le 30/01/2019)



[MATT\\_CRYPTO](#), *Caesar cipher with a shift of 3*, 2014, URL :

[https://commons.wikimedia.org/wiki/File:Caesar\\_cipher\\_left\\_shift\\_of\\_3.svg](https://commons.wikimedia.org/wiki/File:Caesar_cipher_left_shift_of_3.svg) (visité le 30/01/2019), cit. pp. 28, 29.



[NASSIRI, Alessandro](#), *Enigma*, 2012, URL :

[https://commons.wikimedia.org/wiki/File:Enigma\\_\(crittografia\)\\_-\\_Museo\\_scienza\\_e\\_tecnologia\\_Milano.jpg](https://commons.wikimedia.org/wiki/File:Enigma_(crittografia)_-_Museo_scienza_e_tecnologia_Milano.jpg) (visité le 30/01/2019), cit. pp. 28, 29.

## COLOPHON

Ce document a été créé avec  $\text{\LaTeX}$  et  $\text{\BibLaTeX}$ ,  
généré par  $\text{\LuaTeX}$  et édité sous GNU  $\text{\EMACS}$  avec  $\text{\AUCTeX}$ .  
Le texte est composé en *Libertinus Sans* et en *Libertinus Serif*.  
Le code source est composé en *Iosevka*.