

Chiffrer ses e-mails avec GPG

Présentation

Dans le cadre du *Festival des libertés numériques*
30 janvier 2019

Leo Vivier
leo.vivier@gmail.com

C16 PGP

88A6 78C3 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 ».

1/36

Leo Vivier

Chiffrer ses e-mails avec GPG

Table des matières

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

2/36

Leo Vivier

Chiffrer ses e-mails avec GPG

Introduction

1. Introduction

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

2. Chiffrement symétrique

3. Chiffrement asymétrique

4. GPG : Explication

3/36

Leo Vivier

Chiffrer ses e-mails avec GPG

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

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

4/36

Leo Vivier

Chiffrer ses e-mails avec GPG

Bornes de la présentation

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.

5/36

Leo Vivier

Chiffrer ses e-mails avec GPG

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**
 - 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

6/36

Leo Vivier

Chiffrer ses e-mails avec GPG

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·e réel·le du message
 - On **authentifie** la communication

7/36

Leo Vivier

Chiffrer ses e-mails avec GPG

Chiffrement symétrique

1. Introduction

2. Chiffrement symétrique

- 2.1 Vocabulaire
- 2.2 Les bases
- 2.3 Deux exemples
- 2.4 Cas pratique
- 2.5 Les limites du chiffrement symétrique

3. Chiffrement asymétrique

4. GPG : Explication

8/36

Leo Vivier

Chiffrer ses e-mails avec GPG

Vocabulaire

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>	* décrypter
texte clair	<i>plaintext</i>	
texte chiffré	<i>ciphertext</i>	

9/36

Leo Vivier

Chiffrer ses e-mails avec GPG

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

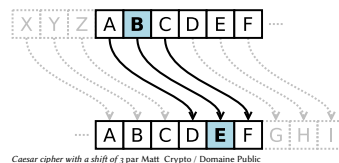
- On le **verrouille** avec une clé
- On le **déverrouille** avec la **même** clé

10/36

Leo Vivier

Chiffrer ses e-mails avec GPG

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

11/36

Leo Vivier

Chiffrer ses e-mails avec GPG



Enigma par Alessandro Nassiri / CC BY-SA-4.0

12/36

Leo Vivier

Chiffrer ses e-mails avec GPG

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

13/36

Leo Vivier

Chiffrer ses e-mails avec GPG

Un grand problème

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

14/36

Leo Vivier

Chiffrer ses e-mails avec GPG

Chiffrement asymétrique

1. Introduction

2. Chiffrement symétrique

3. Chiffrement asymétrique

- 3.1 Les bases
- 3.2 Analogie
- 3.3 Retour au réel

4. GPG : Explication

15/36

Leo Vivier

Chiffrer ses e-mails avec GPG

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

16/36

Leo Vivier

Chiffrer ses e-mails avec GPG

Sophie et Marc

- 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

17/36

Sophie et Marc (cont.)

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**)

18/36

Deux conclusions

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

19/36

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**

20/36

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**

21/36

Leo Vivier

Chiffrer ses e-mails avec GPG

GPG : Explication

1. Introduction

2. Chiffrement symétrique

3. Chiffrement asymétrique

4. GPG : Explication

- 4.1 Clé privée & clé publique
- 4.2 Explication de l'algorithme

22/36

Leo Vivier

Chiffrer ses e-mails avec GPG

Sophie et Marc

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

Chaque paire comporte :

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

23/36

Leo Vivier

Chiffrer ses e-mails avec GPG

Clé privée & clé publique

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 **perdue** ou **volée**, l'**accès** à l'objet qu'elle protège et sa **sécurité** sont remis-e-s en question

24/36

Leo Vivier

Chiffrer ses e-mails avec GPG

Clé privée & clé publique (cont.)

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

25/36

Exemple de clé virtuelle

```
1 -----BEGIN PGP PUBLIC KEY BLOCK-----
2
3 mQINBFA1+ugBEADuozPjHs6+ME9Wm3c94IqqUhwEEFJ3xz1sYJus4V8GMW9TEy1L
4 iQGwx5p1+6yO1+D/tvW3q9jmerdl+EWvQeUvrwkx6r4razTZTe1+48u8jhko85SM
5 xDzEF9wf2gGEt0abZamUu86kfMcmPFMVoGLOI/7feAscP4iGMK9Z1X+C/1wzq20
6 gujhxXdmv7QoYvI17wJRPm4NZHM2MuxLxwxhjifb8JZPE0WGYUJ5+fSPereh0MgC0
7 R53Eo6wIzTU4cBB/dyabI/2/jn2Ya0svoC9B1M8N9mG/bxSqTETiQrgcA1bk0zHj
8 qiY4fXImi+Gkacbzvrdad9QkRVCHSKu/pN6iqZiUvXvfmA0bjRYsoY3JPfjGCTyF
9 58ZELfHnGx6MQtf6Dj0wX7qMBY0jh00n0znmwVp1Mm5Augs6hAvX8Vf99KQVtc
10 mEUnb+Gxc7Y2MBFjWvTpiVvcXAZt8z13gE6UP1s+X5JKdQLqCLR2cq82+EBtS0
11 8U7j00acGGCU3+2/fl8T4KGv1XnUN50nqCb21m076dEsHi2k8016/XPocaLSxzQF
12 ZVRcLsmvD1hct367+mxrrvANmnl7Yy1jGzjzs0fMv5duxnpVpbLFRYz0g4BC2wMb
13 H1KtLFc+b1XkVmvICax+OTE8bP+Yo01qW2gk86wUvjAyebuuxwJXF59XmwARAQAB
14 tDZUVV1scYBzeXN0ZW0gYWRtaW5pc3RyYXRvcnMgPHRhaWxzLXN5c2FkbWluc0Bi
15 b3VtLm9yZz6JAj4EEwECACGFA1A1+ugCGwMFCQPCZwAGCwkIBwMCBhUIAgKCCwQW
16 AgMBAh4BAheAAoJEHD08DEWU190jNEP/RnRhbW30AsMEKptsZmUg09jUAoeWiug
17 Yr5uZ8aiQGTYnTh08wzHKROimPvZ7Ctaszo1q20/VAcdocZDcRD5bmDXgsHFPek0
18 sKcBGAe+pa0tiF0up1rLxcB1MPz7bUCvTn5AMin31hFzLTdq5ei6AK0itaG0Kn5v
19 /E066gsGVJ+edxfMbi+vI0a+cf3bIo1gaPerGUQJKahZUKstwsxiXaucZ1QePdq
20 Yj1zt6XhLe+xvHPN04XWucI1hXm/8RHZcxTbhkt1+kXpIALBjewWraHTgtgP0mmXG
21 MDV00bE3qp1Xxv2451mRu3ypJ6otjq1wo8fPMAgus/3wEn1VUrsYgTR2gUzXVc1
22 ...
```

26/36

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
 - >= 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*

27/36

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** » ?

28/36

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**

29/36

Leo Vivier

Chiffrer ses e-mails avec GPG

Remarque sur l'anonymat

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

30/36

Leo Vivier

Chiffrer ses e-mails avec GPG

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

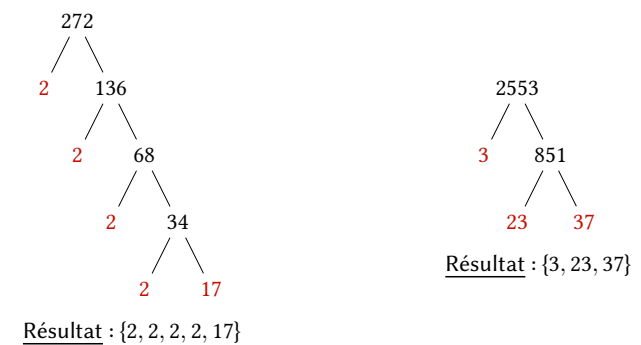
La **cryptographie asymétrique** est basée sur la création de **problèmes mathématiques difficiles** à résoudre dans un *sens* mais **facile** dans un autre

31/36

Leo Vivier

Chiffrer ses e-mails avec GPG

Exemple : Décomposition en nombres premiers

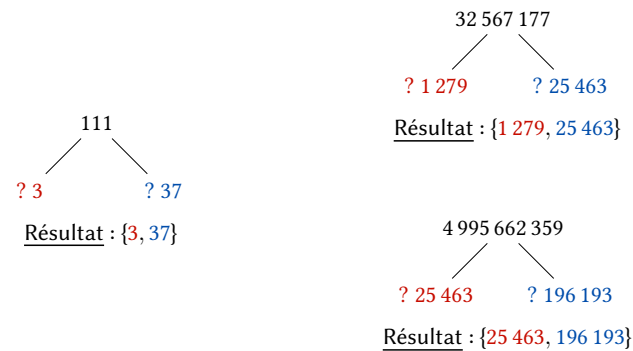


32/36

Leo Vivier

Chiffrer ses e-mails avec GPG

Une difficulté croissante



33/36

Observations

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*

34/36

Retour à l'algorithme

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

35/36

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*^a 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*

36/36

Pour aller plus loin

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 (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)

1/3

Références



MATT_CRYPT0, *Caesar cipher with a shift of 3*, 2014, URL :

https://commons.wikimedia.org/wiki/File:Caesar_cipher_left_shift_of_3.svg (visité le 30/01/2019), cit. p. 13.



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. p. 13.

2/3

Informations supplémentaires

COLOPHON

Ce document a été créé avec L^AT_EX et BibL^AT_EX,
généré par X_YL_AT_EX et édité sous GNU EMACS avec AUCTION.
Le texte est composé en *Libertinus Sans* et en *Libertinus Serif*.
Le code source est composé en *louseka*.

3/3