Présentation succincte sur le chiffrement

Jonas FERNANDEZ - ©ⓘ€=

3 mars 2017

Présentation réalisée avec LaTeX .

Plan de la présentation

- Quelques définitions et généralités,
- Un peu d'histoire, de César à Enigma
- Principes des chiffrements symétrique et asymétrique
- RSA (1977)
- Création de PGP (1991)
- Deux exemples : GnuPG (Asymétrique) et Veracrypt ou TrueCrypt (Symétrique).

Définitions

- Chiffrement : Transformer un texte clair en texte codé à l'aide d'une clé ou d'un secret,
- Le déchiffrement : Utilisation d'une clé ou d'un secret pour accéder en clair à un texte chiffré.
- Décryptage : Restitution d'un texte clair à partir d'un texte chiffré, par des moyens de cryptanalyse.
- Clé : Secret partagé (sous forme de texte ou de fichier) permettant de chiffrer ou de déchiffrer un document.
- Cryptanalyse : Discipline permettant de décrypter des documents grâce à des procédés mathématiques.
- Histoire de serrure ou de porte...

Pourquoi chiffrer ?

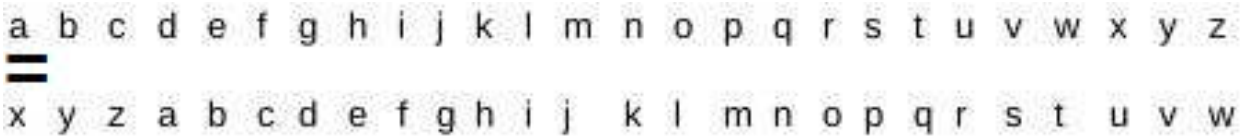
- Pour sécuriser vos échanges sur Internet. Vous utilisez parfois le chiffrement sans vous en rendre compte.
- Mais à part çà ? Vous pensez vraiment que vous n'avez rien à cacher ?
- Prism alias US-984XN : 

,
- Espionnage industriel,
- Protection de la vie privée,
- Amélioration de la sécurité et de la confidentialité des données,
- Piratage des messages d'Hillary,
- Défenseurs des droits de l'homme, journalistes dans certains pays (VPN, Messagerie chiffrée),
- Secret médical,
- Jusqu'à la fin du 20^{ieme} siècle, un courrier sous enveloppe fermé était à peu près sûr. Mais maintenant ?

Chiffrement César

Le chiffrement par décalage

- Le chiffrement de César consistait à décaler les lettres de l'alphabet.



- "Hello World" devient "Ebiil tloia" avec une clé égale à 3.
- En l'absence de la clé (Dans l'exemple, c'est 3), il faut utiliser des techniques basiques de cryptanalyse...
- Analyse fréquentielle ou analyse de fréquence.
- méthode d'analyse inventée par un hacker irakien qui s'appelait Al Kindi et vivait à Bassora...
- ...il y a environ 1200 ans.

Autre exemple de chiffrement

- CFFIHC ORAEEE NEOICL FMRAYR EENTLU RENCES
- solution . . .

C	F	F	I	H	C
O	R	A	E	E	E
N	E	O	I	C	L
F	M	R	A	Y	R
E	E	N	T	L	U
R	E	N	C	E	S

- Ici, la clé est le point de départ et le sens de la spirale.
- CONFERENCE SUR LE CHIFFREMENT LYCEE AORAI
- Utilisation de la géométrie, d'un tableau de lettres, etc.

Le chiffre de Vigenère

La renaissance

- Besoin de renforcer la confidentialité des correspondances diplomatiques,
- Cette technique décrite par Vigenère en 1586 existait déjà depuis plusieurs décennies,
- Et elle a tenu plusieurs siècles avant d'être cassée par un sous-officier prussien en 1863,
- Elle rend caduque la technique inventée par notre hacker irakien il y a 1200 ans,

Table de Vigenere

- Le principe était simple. Une phrase et une clé répétée plusieurs fois.
- Phrase : La cryptographie, c'est bien
- Clé : ch ouettechouett, e'cho uett (Chouette répété x fois)
- résultat : A vous de jouer...

Table de Vigenère.

Clé utilisée	Lettre en clair																								
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	26 lettres chiffrées																									
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Indice de coïncidence

Notion complexe qui fait appelle aux mathématiques et qui finalement ressemble un peu à l'analyse fréquentielle.

- Chaque langue a un indice de coïncidence propre pour l'apparition de l'ensemble des lettres dans un message.
- Permet aux cryptanalystes de vérifier s'ils ont affaire à un texte intelligible.
- S'ils s'éloignent trop de l'IC, ils savent qu'ils sont sur la mauvaise voie.
- La signature IC d'un texte en français est 0,0746
- La signature IC d'un texte écrit avec des lettres aléatoires est de 0,038
- Création du procédé : aux alentours de 1920.
- Une formule mathématique : $IC = \sum_{q=A}^{q=Z} \frac{n_q(n_q-1)}{n(n-1)}$ ...Sans commentaire.
- Permet de déterminer la longueur de la clé avec un chiffrement de type Vigenere.

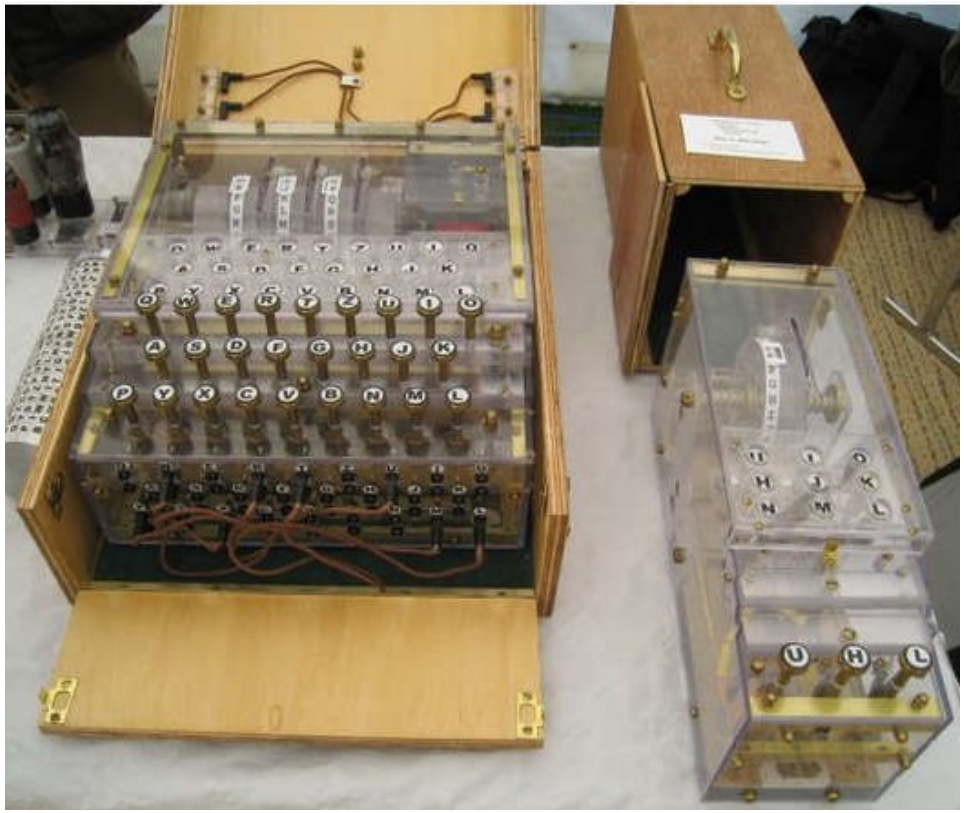
Enigma le coté obscur de la cryptographie.

Comment la cryptanalyse a sauvé le monde.

- Enigma était une machine électromécanique portative permettant de chiffrer ou de déchiffrer des informations. Il en a existé plusieurs versions. L'invention date de 1919.
- Les clés de chiffrement sont des instructions de montage des rotors (brouilleur) et de la connexion de câbles du tableau de permutations
- Un film conseillé : "Imitation game" qui raconte une partie de la vie d'Alan TURING, génie des mathématiques et quasiment inventeur de l'informatique.

- un système de chiffrement mal utilisé est faillible. Les nazis ont commis des erreurs. Lesquelles ?
- La cryptanalyse a permis d'écourter la guerre d'au moins deux ans.
- On comprend pourquoi la cryptographie est considérée comme une arme.

Enigma en images



Et en chiffre : environ 1,59 x 10^{20} possibilités de chiffrement. Il faut avoir un peu de temps libre pour en venir à bout !
Et le réglage changeait tous les jours !

Symétrie – Asymétrie

–

- On peut chiffrer de manière symétrique donc avec une seule clé qui sert à chiffrer et déchiffrer.
- Et on peut chiffrer de manière asymétrique, c'est à dire en utilisant une clé publique et une clé privée. Et les choses se compliquent un peu...
- J'ai choisi une vidéo toute faite et assez claire `https://www.youtube.com/watch?v=ln2FmlRUrs8`

RSA

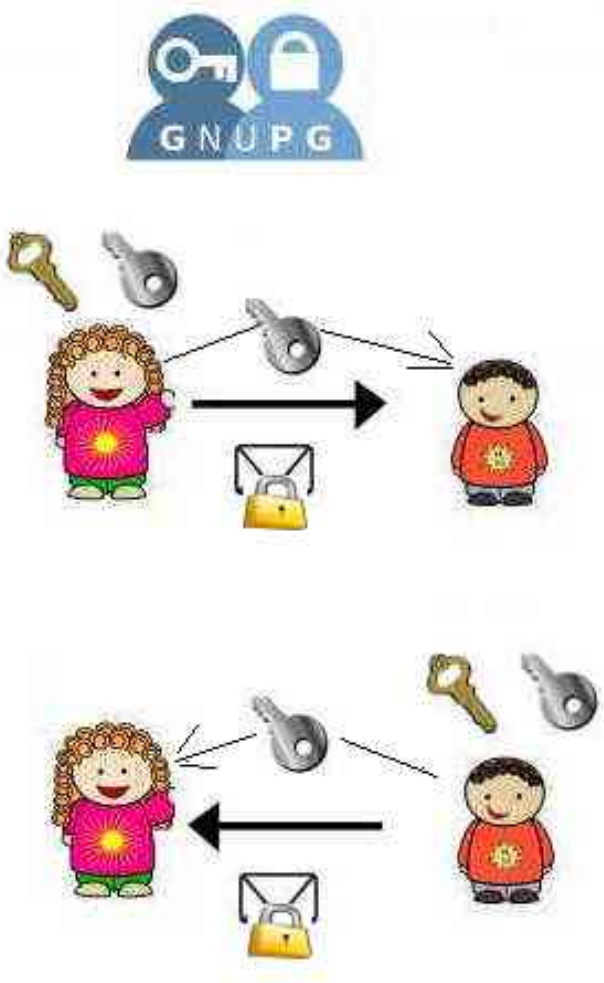
Tous les nombres premiers sont impairs sauf un, tous les nombres premiers sont impairs, sauf 2

—

- RSA (Rivest, Shamir et Adleman) 1977. Pour un grand nombre, il faut trouver les deux facteurs premiers.
- Pour faire simple, j'ai pris pour exemple 6557 qui a pour facteurs : 79 et 83
- 6557 est la clé publique. La clé privée se compose de 79 et 83
- En réalité, c'est un peu plus compliqué que ça...
- La longueur des nombres utilisée est actuellement de 320 bits. Ça n'a pas toujours été le cas.

Clés publiques / clé privée – Exemple

–



Clé privée **A conserver et ne jamais communiquer**

Clé publique **A communiquer de façon sécurisée**
En main propre étant le mieux

```
-----BEGIN PGP MESSAGE-----
Version: GnuPG v2

hQEMA71J5POrhAU3AQgAuVfZPQ2E6i0tnKzALIc0WZJXZEv1CENxq1cgzmXueczr
VAUnl6bt1FdzDOUPhGJyCVdOjPYec8V+a+Bw/xS0iFuRbPzhIgeuA4a4wofcknmG
XP4T6QNhL7nm3ccuPGrBT6iUOV2ZZfdDJAL/vgmYWZOMhoDKN64VXT6dhA1+MnAu
uKuVK97EctK5yfbrmak84LHPB7F3pcWOGC8s9PE5N6m8J/tN5FYMfVXYMJ55L7u0
9MnnkjK5mXmwUrzNwpCFLq1ackStO4REMMIYdz9yXGFKGluCLBiqZXOQG8pSlisF
cHvniiF+Ycmp96ZTse52ySB6V5rC6mcCt9nM8+KB/NLBEQGXgu5qmdMnrlK66+wH
jNUDnfQhrBOPIA64WuemGdnqv3YxZxk9/MvTuSmCok2cdydqFfzAkkneC2OcoIQP
Ks4APpGHGKQzOm4RTA6ccjkI2TTVtQc8fPQJrCIZHVTi2wfxB1dZkUsRs9b+HSXf
8bes+Kl6ONR9jkvDx5Rw6vNHK1IwThbltNp38QtNl4pHqBfP9CgycsSfTVkT4019
5bnVgVMexhagBX80nJsyXZiTlO1KcQXVrmCps7/T/t2Rfmxtu76YqWgkP832hCts
ahhNrdCOKmtylvGvag4J21NRbcPEz6azkCZVxfrPiTysM0Y+aHs/6JW3dCj2fUYL
iK2j2EL/Srvige4U5VuMLzn2n2BHJ3HXE4n0OTRYcqyI7h8qXOZaeY3RDj7qJwP2
31nd40l4fOAB+6psZ5DbRA8uY2oF4vWZiy9pjDWHUiXQVy+TJV++MimdhSZjVtVF
iucUE9V1V+s8SpDBuJ14BgGV1rX7D9/Hq14VuXnxpvj5qo+2VyNp7IEA6OrwD4Vx
diauzLAM6E5MhHRimWBCDMNLPwq07ZaNMvN2cu8IqN4vmEKe8KCwn/UcYuscWI0r
aF16FMfEOlVrJgUggcz5irC8Qg==
=VSap
-----END PGP MESSAGE-----
```

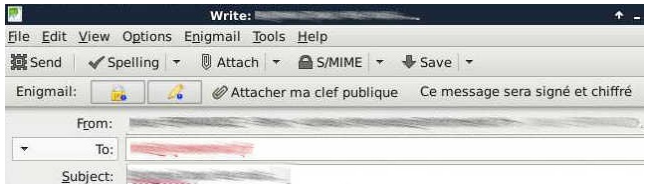
Phil ZIMMERMANN & PGP (Pretty Good Privacy)

- 1991, année extraordinaire :
  - Création du noyau Linux par un étudiant finlandais.
  - Création de PGP par Phil Zimmermann,
- 1993 : Diffusion de PGP en dehors des USA. Mais la loi dite "Arms Export Control Act" de 1976 l'interdisait.
- Des poursuites ont eu lieu en 1993, mais ont été abandonnées 3 ans plus tard. Pourquoi ?
- Peu de temps après, création d'OpenPGP, standard décrit dans la RFC4880 et dérivé du logiciel PGP.
- GnuPG (Gnu Privacy Guard) a été créé à la fin des années 1990, c'est un produit concurrent de PGP et c'est un logiciel libre.

GnuPG et Enigmail

Enigma pour le mail, mais en mieux

—

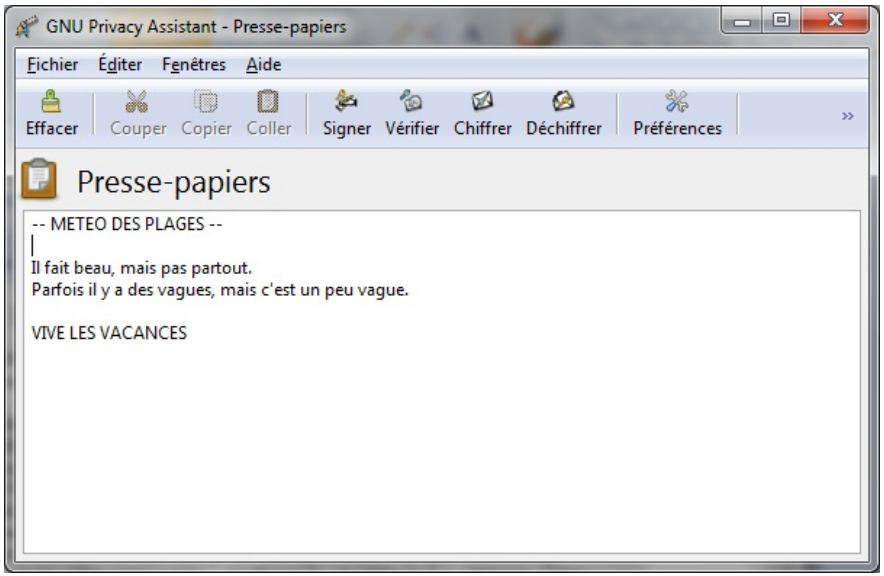


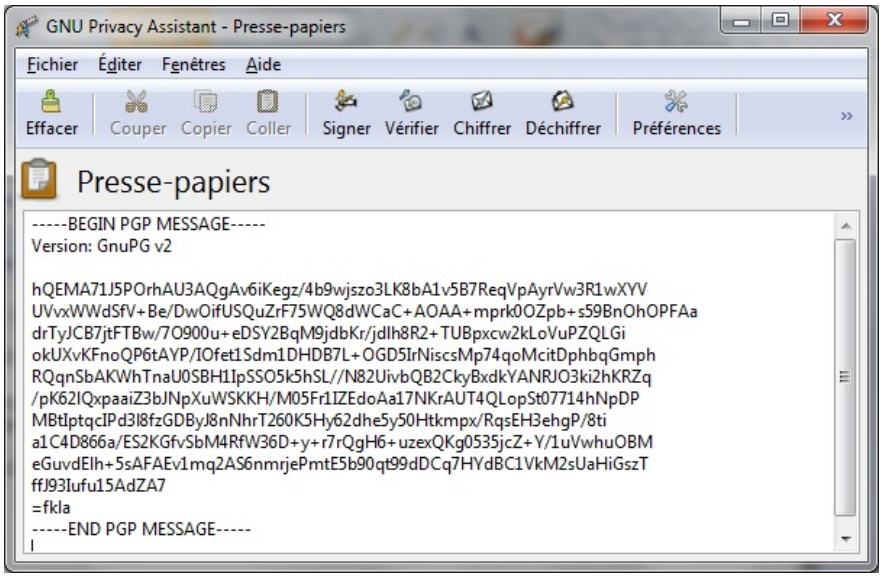
- Enigmail est un module de chiffrement et de signature de courrier électronique (Thunderbird, seamonkeys, Icedove, etc.)
- Les fonctions de chiffrement d'Enigmail sont assurées par GnuPG.
- Si vous utilisez un webmail, vous devrez chiffrer vos messages séparément. (gpg sur les systèmes de type UNIX, ou Gnu Privacy Assistant sur les systèmes à courant d'air).
- Si Hilary Clinton avait utilisé Enigmail, . . .
- Enigmail est libre et gratuit, il propose un chiffrement fort, est multiplateforme.
- Inconvénient : il n'y a pas de tiers de confiance, donc il faut échanger les clés publiques de façon strictement sécurisées.

GPG et Gnu Privacy Assistant

Chiffrement de fichier ou de texte

- Sous Windows il faut installer GPG4Win





Sous Gnu/Linux, Mac OS/X et les autres systèmes Unix, installer gpg.

Veracrypt

Chiffrement de stockage

–

- Veracrypt permet de créer des containers de stockage sous forme fichiers.
- Il permet également de chiffrer intégralement des supports tels que des clés USB ou des disques durs.
- une petite démo...

Quelques pistes pour approfondir

—

- http://www.apprendre-en-ligne.net/crypto/menu/index.html
- https://fr.wikipedia.org/wiki/PRISM_%28programme_de_surveillance%29
  Vous trouverez dans différents journaux beaucoup d'articles sur le sujet.
- Photographies d'Enigma
  http://museeradiomili.com/photos-machine-enigma/
- En français https://www.youtube.com/watch?v=7dpFeXV_hqs