INSA

Chiffrer ses mails avec PGP

Par Gildas Avoine

- Origine
- Alice et Bob
- Crypto symétrique et asymétrique
- Création d'une clef
- Certification de la clef

INSA

Introduction

Proposé en 1991 par Philip Zimmermann (État-Unis)

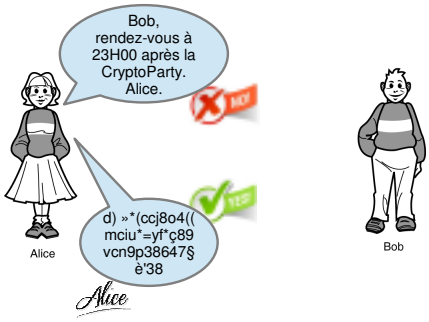
Objectif : protéger les communications électroniques

Chiffrement et signature des mails

Logiciel, Standard (OpenPGP)

INSA

Alice et Bob

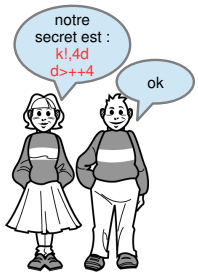


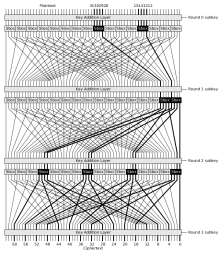
Source des images : http://vamban.ru/

Cryptographie symétrique

Cryptographie symétrique, dite à clef secrète

Alice et Bob partage un secret commun





Source des images : http://www.cs.rit.edu/~ark

Cryptographie asymétrique

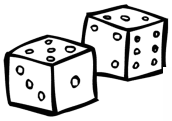
Cryptographie asymétrique, dite à clef publique

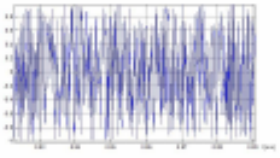
Chacun possède une paire (clef publique, clef privée)

Génération des clefs

Les clefs doivent être autant aléatoire que possible

La clef privée être protégée sur la machine





Source des images : www.dididou.fr et public.utenligne.net

Certificats

Il faut être certain d'utiliser la bonne clef !

Tout le monde peut certifier (signer) des clefs, serveurs.

Ne pas perdre ses clefs !

Mise en pratique

1. Installer un logiciel
2. Récupérer clef publique de cryptoparty@laposte.net
   → Sur le site http://pgp.mit.edu/
3. Envoyer un message chiffré à cryptoparty@laposte.net
4. Générer d'une paire de clefs
   → Mettre date de validité et faire un cert. de révocation
   → Utilisateur anonyme
5. Diffuser sa clef publique sur http://pgp.mit.edu/
6. Envoyer message chiffré/signé à une personne dans salle
7. Signer la clef publique d'un autre personne dans salle

Logiciels

	Linux	Windows	Mac OS
Logiciel	GPA, GnuPG	GPG4Win	GPGTools
Plug-in Navigateur	Mailvelope (firefox, Chrome), WebPG (Firefox, Chrome)	Mailvelope (firefox, Chrome), WebPG (Firefox, Chrome)	Mailvelope (firefox, Chrome), WebPG (Firefox, Chrome)
Plug-in Client Messagerie	Enigmail (Thunderbird)	Enigmail (Thunderbird)	Enigmail (Thunderbird)

https://www.gnupg.org/related_software/frontends.html