Cryptographie et sécurité

Guillaume Lecoquierre
« Skhaen »

skhaen@cyphercat.eu

PSES 2012

Ce que nous allons voir

- Les bases de la cryptographie,
- pourquoi se protéger,
- des exemples,
- encore des exemples.

$$\left(\left(\frac{x}{7}\right)^2\sqrt{\frac{\left|\left|x\right|-3\right|}{\left|x\right|-3}}+\left(\frac{x}{3}\right)^2\sqrt{\frac{\left|y+\frac{3\sqrt{33}}{7}\right|}{y+\frac{3\sqrt{33}}{7}}}-1\right)\cdot\left(\left|\frac{x}{2}\right|^{\smile}\left(\frac{3\sqrt{33}-7}{112}\right)x^2-3+\sqrt{1-\left(\left|\left|x\right|-2\right|-1\right)^2}-y\right)$$

$$\cdot\left(9\sqrt{\frac{\left|\left(\left|x\right|-1\right)\left(\left|x\right|-.75\right)\right|}{\left(1-\left|x\right|\right)\left(\left|x\right|-.75\right)}}\right)\cdot\left(3\left|x\right|+.75\sqrt{\frac{\left|\left(\left|x\right|-.75\right)\left(\left|x\right|-.5\right)\right|}{\left(.75-\left|x\right|\right)\left(\left|x\right|-.5\right)}}-y\right)$$

$$\cdot\left(2.25\sqrt{\frac{\left|\left(\left|x\right|-1\right)\left(\left|x\right|-.75\right)\right|}{\left(1-\left|x\right|\right)\left(\left|x\right|-.75\right)}}\right)\cdot\left(\frac{6\sqrt{10}}{7}+\left(1.5^{\smile}.5\left|x\right|\right)\sqrt{\frac{\left|\left|x\right|-1\right|}{\left|x\right|-1}}^{\smile}\frac{6\sqrt{10}}{14}\sqrt{4-\left(\left|x\right|-1\right)^2}-y\right)=0$$

Ce que nous ne verrons pas

$$\left(\left(\frac{x}{7}\right)^2\sqrt{\frac{\left|\left|x\right|-3\right|}{\left|x\right|-3}}+\left(\frac{x}{3}\right)^2\sqrt{\frac{\left|y+\frac{3\sqrt{33}}{7}\right|}{y+\frac{3\sqrt{33}}{7}}}-1\right)\cdot\left(\left|\frac{x}{2}\right|^{\smile}\left(\frac{3\sqrt{33}-7}{112}\right)x^2-3+\sqrt{1-\left(\left|\left|x\right|-2\right|-1\right)^2}-y\right)$$

$$\cdot\left(9\sqrt{\frac{\left|\left(\left|x\right|-1\right)\left(\left|x\right|-.75\right)\right|}{\left(1-\left|x\right|\right)\left(\left|x\right|-.75\right)}}\right)\cdot\left(3\left|x\right|+.75\sqrt{\frac{\left|\left(\left|x\right|-.75\right)\left(\left|x\right|-.5\right)\right|}{\left(.75-\left|x\right|\right)\left(\left|x\right|-.5\right)}}-y\right)$$

$$\cdot\left(2.25\sqrt{\frac{\left|\left(\left|x\right|-1\right)\left(\left|x\right|-.75\right)\right|}{\left(1-\left|x\right|\right)\left(\left|x\right|-.75\right)}}\right)\cdot\left(\frac{6\sqrt{10}}{7}+\left(1.5^{\smile}.5\left|x\right|\right)\sqrt{\frac{\left|\left|x\right|-1\right|}{\left|x\right|-1}}^{\smile}\frac{6\sqrt{10}}{14}\sqrt{4-\left(\left|x\right|-1\right)^2}-y\right)=0$$

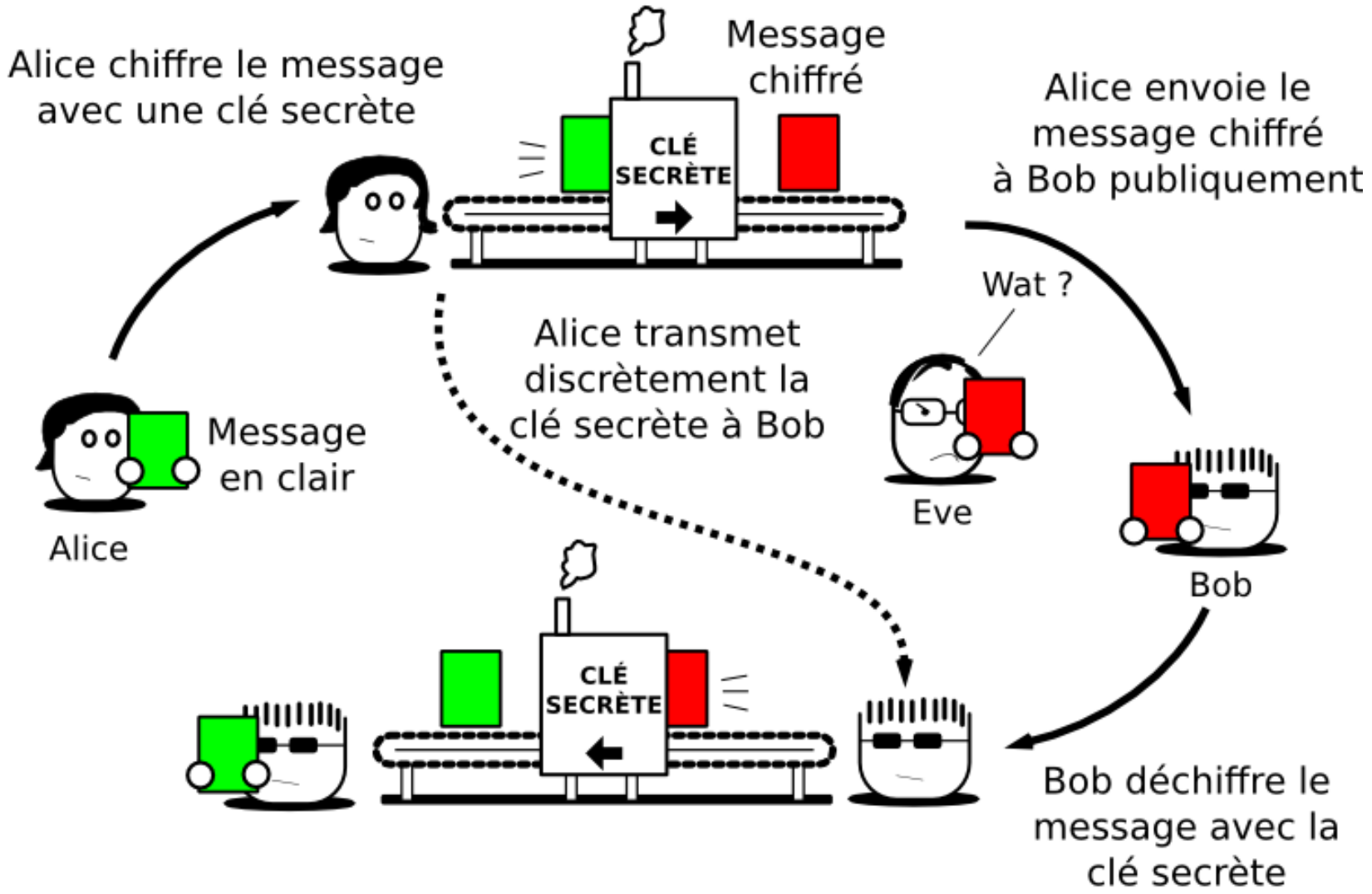
Vocabulaire

- **chiffrer** : « coder » le texte en clair, grâce à la clé, pour produire un texte chiffré (*encryption* en anglais),
- **déchiffrer** : « décoder » (retrouver le texte en clair) quand on connaît la clé (*decryption* en anglais),

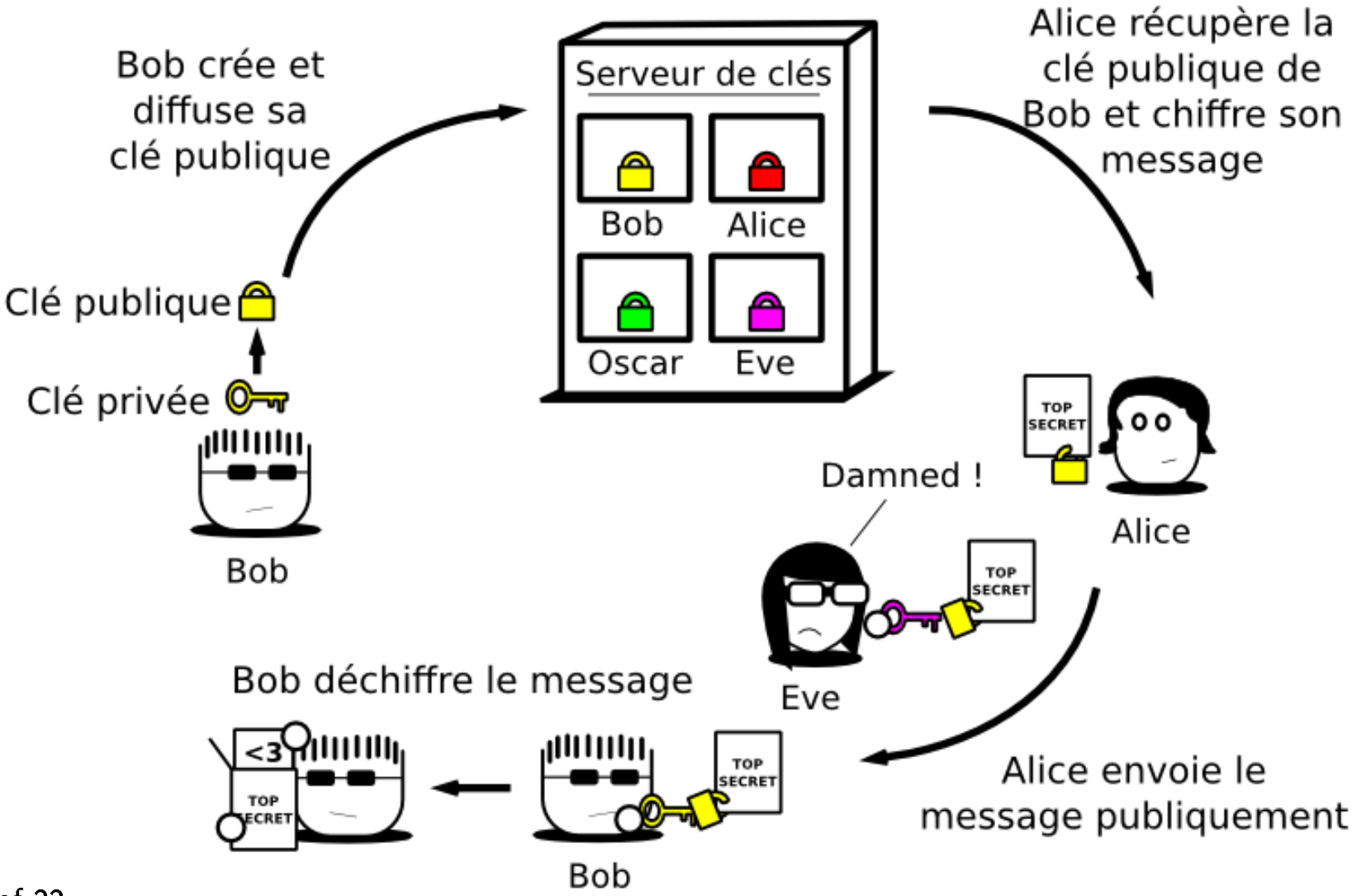
---

- **décrypter** : « décoder » quand on ne connaît pas la clé,
- **crypter** : n'existe pas, tout simplement.

Chiffrement symétrique



Chiffrement asymétrique



hachage (hash)

Fonction à sens unique permettant le « calcul » d'une empreinte.

- **sha256sum** Nous venons en paix.

9d6bd655e000f83685d64affde380a3d94a62d47d42d80a0be11a4bb4c6ee324

- **sha256sum** Nous venons en paix

dc94694324e4df8cbda29db6e98778a29254ffa8040a2e99855bcd19e4b3c1c6

Empreinte - exemples

- **MD4/MD5** (128 bits), **SHA-0** (160 bits) :obsolète (collision totale),
- **SHA-1** (160 bits) : dangereux depuis 2005,
- **SHA-2** (224, 256, 384, 512 bits) : standard actuel,
- **SHA-3** : en cours de réalisation,
- **RIPEMD** : obsolète (collision complète / août 2004),
- **RIPEMD** (128/160/256/320) : pas de problème connu,
- **TIGER** (192, 128 et 160 bits) : des attaques ont été trouvé,
- **Whirlpool** (512 bits) : standard actuel.

Vérification

- **Empreinte** (idéale pour les soirées) :
  - 0102 e489 769b 9189 5107 330c 3307 0e51 0e6d 2522 d091 804d eec4 210d f291 b61e 8dd6
- **secret partagé** (mot de passe),
- **QrCode** (pour textsecure par exemple),
- question / réponse,
- papiers d'identité (keysigning party).

Libre / open-source

- logiciel gratuit (freeware / gratuiciel) : skype, ultrasurf ...
- **logiciel libre** (free software) : Mumble, Tor, VLC ...

Quand on parle de cryptographie et d'(h)ac(k)tivisme, cette différence peut sauver des vies.

Un bon système cryptographique est :

- **open-source**,
- massivement **utilisé**,
- **audité** par des programmeurs, des experts et des chercheurs.

Vous avez dit stupide ?

Application Android « *Skyrim Game Wallpaper* » par U.S.KANHAIYA

- **Appeler** directement un numéro de téléphone,
- Contrôle du matériel : **enregistrer un fichier audio**,
- **Position géographique approximative**,
- **Accès internet intégral**,
- **Lire l'historique** et les favoris du navigateur,
- **modifier l'historique** et les favoris du navigateur,
- **lire l'état** et **l'identité du téléphone**.

Le cas « *Cryptweet* »

Chiffrement des messages privés pour twitter avec un « chiffrement fort », plus de détails sur `http://plexusproject.org`

- mauvaise implémentation / erreurs de développement :
  - pas d'accès en HTTPS au serveur de clé public.
  - utilisation de DES3 avec des mauvais paramètres pour la clé privé,
  - utilisation de RSASSA-PKCS1-v1_5 pour la signature, à la place de RSAES-PKCS1-v1_5.

« *Just copy and paste a PGP encrypted message to pastebin.ca and and tweet the link, if you must* »

Vous avez dit dangereux ?

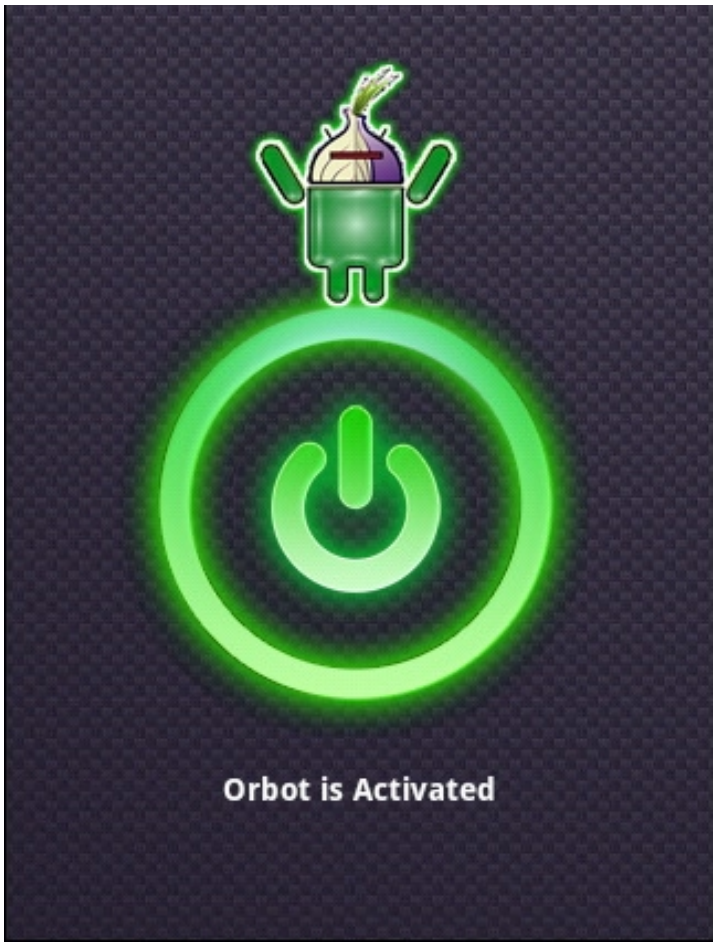
- **Skype** : backdoor pour les autorités par Microsoft. Chiffrement ? Sécurité ?
- **Ultrasurf** : trojan (syrie), code malveillant.
- **XMPP par facebook** : serveurs de facebook, modification des urls.
- **BlackBerry / Iphone**

TextSecure

- Stock vos sms (reçu et envoyé) en local (AES-128).
- Les sms sont chiffrés avec **OTR** si votre interlocuteur dispose lui aussi de TextSecure.

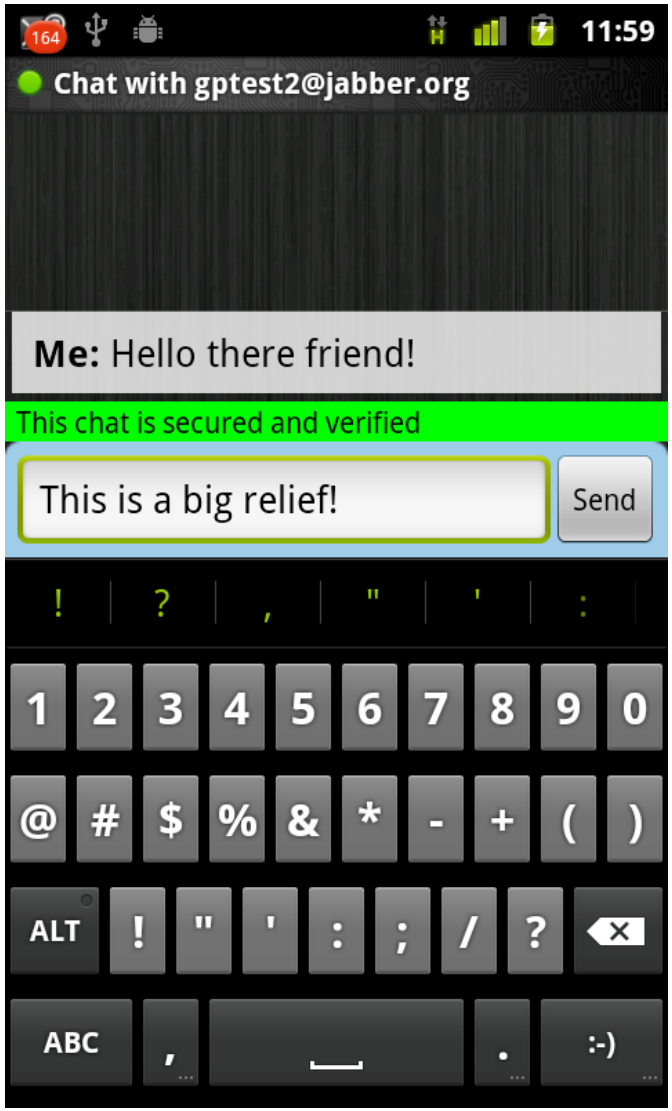
Orbot

- permet de passer via le réseau **TOR**.



GibberBot

- Application de messagerie instantanée (**XMPP**),
- contourne les firewalls et les filtrages (via **Orbot** / TOR),
- chiffrement point-à-point via **OTR**.



cSIPsimple / OSTel

- OSTN - Open Secure Telephony Network
- Chiffrement : SRTP, ZRTP, SIP TLS

InTheClear

- **Emergency SMS** : permet d'envoyer un sms préécrit à une liste de contacts préenregistré.
- **Data Wipe** : - / contacts / photos / appels / sms / calendrier / carte SD.

Logiciels

- **Mails** : GPG,
- **VOIP** : cSIPsimple, Jitsi, I Hear U, SFLphone, ... Mumble,
- **Proxy / Anonymat** : TOR, I2P,
- **Messagerie instantanée** : xmpp + OTR, TorChat,
- **Chiffrement** : LUKS, TrueCrypt, VPN ...

Android

- **SMS** → TextSecure,
- **VOIP** → OSTel, cSIPsimple,
- **Messagerie instantanée** → GibberBot (XMPP + OTR + Orbot),
- **Proxy / Anonymat** → Orbot (Tor),
- **GPS** → DroidTracker,
- **Système** → InTheClear,
- **Chiffrement** : VPN ...

Et maintenant ?