Chiffrement asymétrique

Éric BERTHOMIER
eric.berthomier@free.fr

6 juin 2023

Version 1.1 - Version Stagiaire

Rappel sur le chiffrement

Objectif protéger la confidentialité de messages entre leur émetteur et leur destinataire.

Rappel sur le chiffrement

Objectif protéger la confidentialité de messages entre leur émetteur et leur destinataire.

Comment Les premières inventions reposaient sur des procédures secrètes permettant de transformer un message clair en un message incompréhensible pour un attaquant.
La connaissance de cette opération secrète était partagée entre l'émetteur et le destinataire du message.

Chiffrement asymétrique

Un chiffrement asymétrique se base sur la création de 2 clésă:

- Une clé privée pour le chiffrement et le déchiffrement.

Chiffrement asymétrique

Un chiffrement asymétrique se base sur la création de 2 clésă:

- Une clé privée pour le chiffrement et le déchiffrement.
- Une clé publique pour le chiffrement.

Chiffrement asymétrique

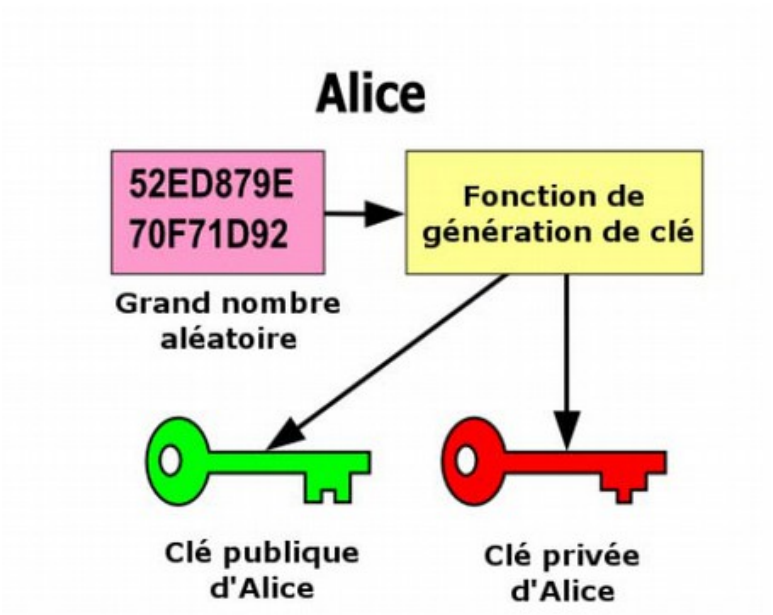
Un chiffrement asymétrique se base sur la création de 2 clésă:

- Une clé privée pour le chiffrement et le déchiffrement.
- Une clé publique pour le chiffrement.

Chiffrement asymétrique

Un chiffrement asymétrique se base sur la création de 2 clésă:

- Une clé privée pour le chiffrement et le déchiffrement.
- Une clé publique pour le chiffrement.



Chiffrement asymétrique : les fondements

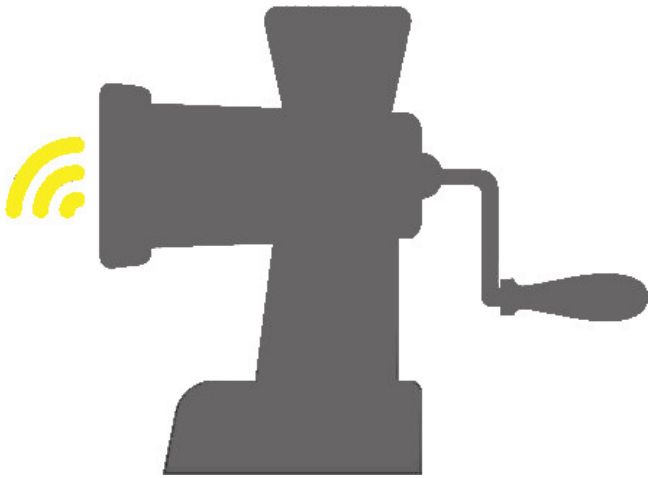
- La clé privée et la clé publique sont liées mathématiquement.

Chiffrement asymétrique : les fondements

- La clé privée et la clé publique sont liées mathématiquement.
- La clé privée peut elle-même être protégée par un mot de passe.

Chiffrement asymétrique : les fondements

- La clé privée et la clé publique sont liées mathématiquement.
- La clé privée peut elle-même être protégée par un mot de passe.
- Il est impossible de retrouver la clé privée à partir de la clé publique.



Chiffrement asymétrique : Exemple de génération des clés

```
ssh-keygen

Generating public/private rsa key pair.
Enter file in which to save the key (/home/eric/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/eric/.ssh/id_rsa.
Your public key has been saved in /home/eric/.ssh/id_rsa.pub.
The key fingerprint is:
SHA256:mZNtbzcE2SO6PLhMOaeBOZZ4LDTNOZYemnegXJWPcOU eric@ERIC-PC
The key's randomart image is:
+---[RSA 2048]----+
|         .. .E   |
|      o +.  o.   |
|     o @  o+.o   |
|    o @ &o.oo .  |
|     B S Bo. .   |
|      = O * .    |
|       o = o o   |
|      o . o . .  |
|       o         |
+----[SHA256]-----+
```

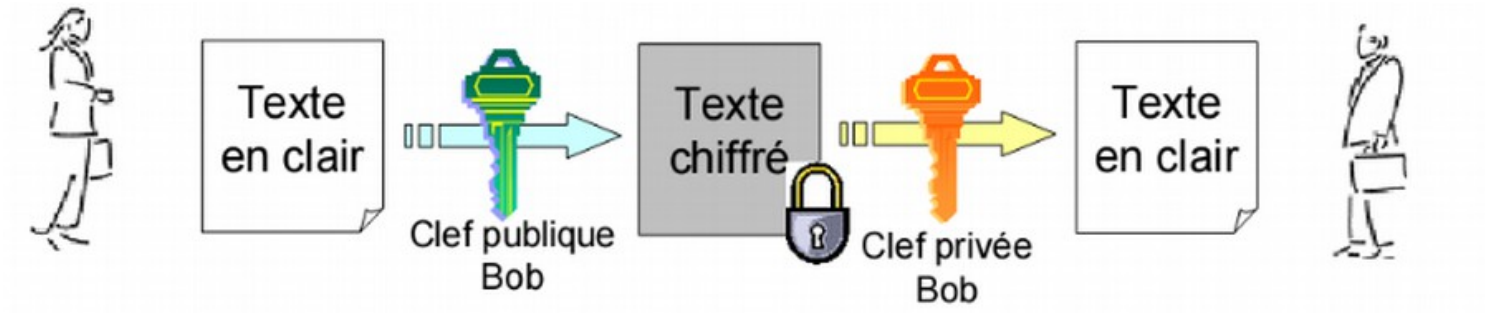
Chiffrement asymétrique : La clé publique dépend de la clé privée

```
ssh-keygen -y -f ~/.ssh/id_rsa > cle_publique.pub
Enter passphrase:

cle_publique.pub
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDf+QD2PLWm+
      YuQvtPHx1UGdCiLA8PAOa973s64ZH1MqO6oMOOlY9JqcjPJnaKPfrlogx/2/kXN0xjD/
      BGbh56m8Lfu3hK7cgVpVfD29gHi+
      PyUhw84dcioXOPC5XAUMMOFdYSLJwJmiIULgXAs6IgfAwMDLlSZ9vSJjcAaFYuiBb1h3fYXeyX9tnAn10aUvH07ydNa6C1
      +HPDAcz929iF8H8MSzKYJoDCNpZejq7KOVC98eRuVXtmZn1ZI3zsBIVjYt25T3TDvknmk0+
      pFznKtnMPjeNaTyGp0C90sN23rE0YgIoVNW3/RjVUCrr1CKVerda+EWD6gwqQ6fodbSNjx

Origine
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDf+QD2PLWm+
      YuQvtPHx1UGdCiLA8PAOa973s64ZH1MqO6oMOOlY9JqcjPJnaKPfrlogx/2/kXN0xjD/
      BGbh56m8Lfu3hK7cgVpVfD29gHi+
      PyUhw84dcioXOPC5XAUMMOFdYSLJwJmiIULgXAs6IgfAwMDLlSZ9vSJjcAaFYuiBb1h3fYXeyX9tnAn10aUvH07ydNa6C1
      +HPDAcz929iF8H8MSzKYJoDCNpZejq7KOVC98eRuVXtmZn1ZI3zsBIVjYt25T3TDvknmk0+
      pFznKtnMPjeNaTyGp0C90sN23rE0YgIoVNW3/RjVUCrr1CKVerda+EWD6gwqQ6fodbSNjx eric@ERIC-PC
```

Chiffrement asymétrique : Clé publique

Chiffrement asymétrique

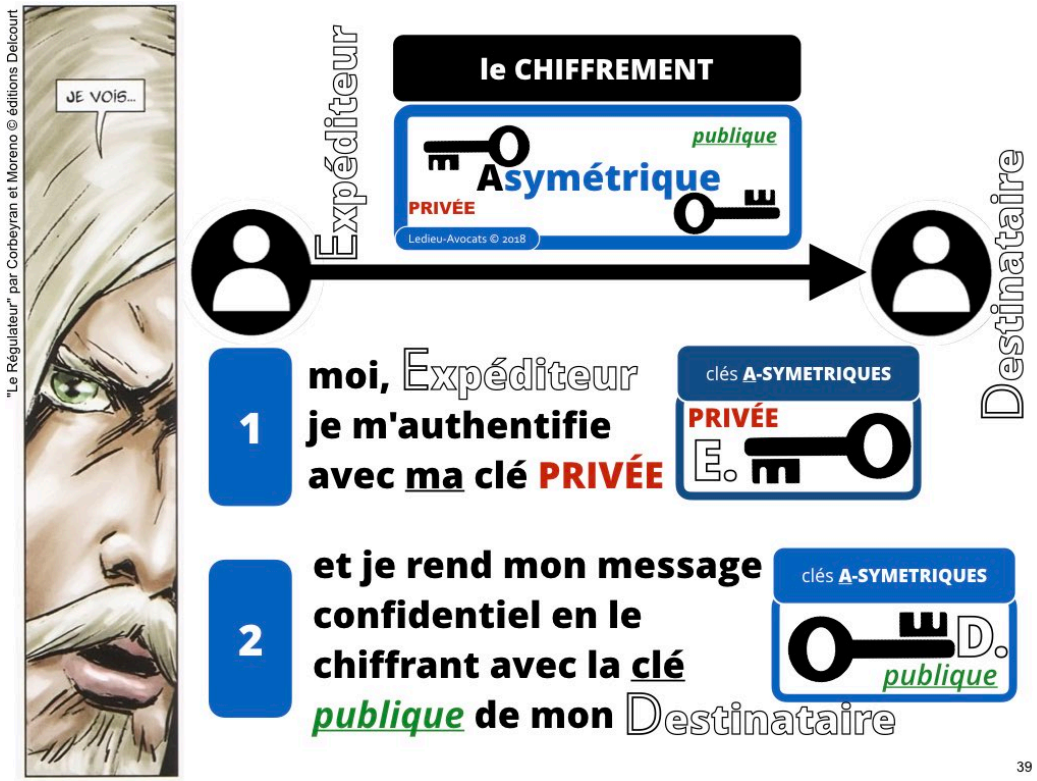
La clé publique d'une personne peut être utilisée pour chiffrer un message à destination du propriétaire de la clé privée



Chiffrement asymétrique : Envoi d'un courriel

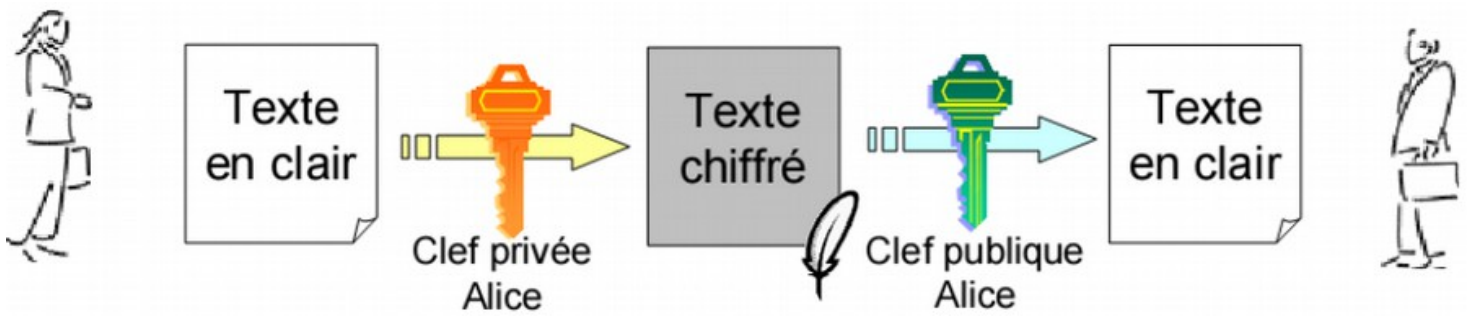
24

Chiffrement asymétrique : Envoi d'un courriel



Chiffrement asymétrique

La clé publique d'une personne peut être utilisée pour contrôler la signature d'un message en provenance d'une personne.

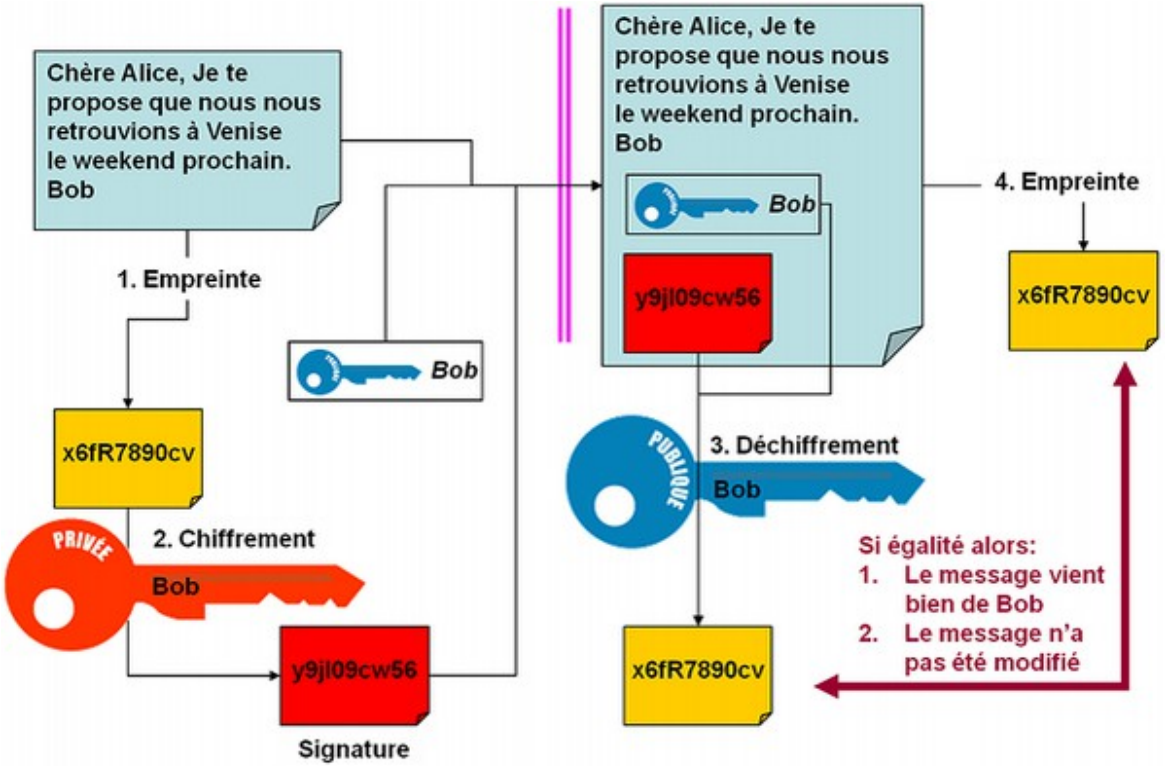


Chiffrement asymétrique : Signature électronique

28

Chiffrement asymétrique

Dansălaăpratique,ăl'algorithmeăest appliqué au condensat du message.



Chiffrement asymétrique : Le BitCoin

CHIFFREMENT | **procédure pénale**

jurisprudence 2018
des services d'enquêtes judiciaires

Ledieu-Avocats © 2018

le détenteur de la clé privée est réputé détenteur du compte BitCoin litigieux

27 juin 2018

Capitaine Édouard KLEIN
docteur en informatique, enquêteur criminaliste - Centre de lutte contre les criminalités numériques de la gendarmerie nationale

atelier de recherche de la gendarmerie
BLOCKCHAIN : la sécurité absolue ?

Les certificats numériques

- La clé privée de l'autorité de certification sert à signer numériquement le hashage des informations contenues dans le certificat.

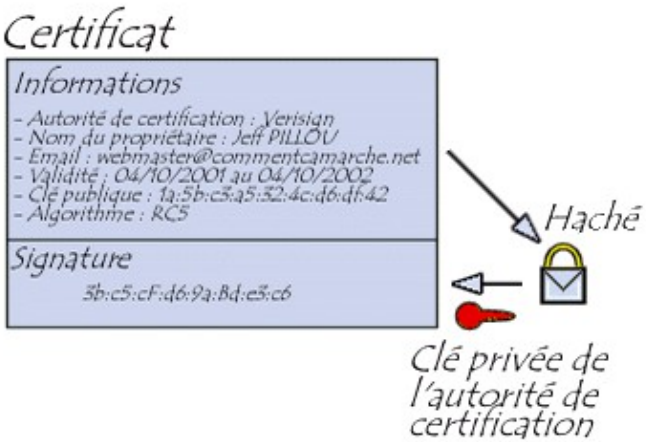
Les certificats numériques

- La clé privée de l'autorité de certification sert à signer numériquement le hashage des informations contenues dans le certificat.
- La clé publique de l'autorité de certification est utilisée pour vérifier le contenu du certificat.

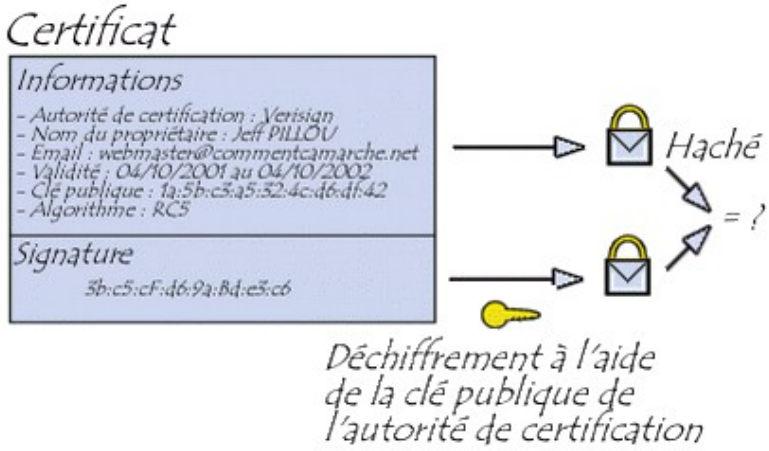
Les certificats numériques

- La clé privée de l'autorité de certification sert à signer numériquement le hashage des informations contenues dans le certificat.
- La clé publique de l'autorité de certification est utilisée pour vérifier le contenu du certificat.
- Le certificat contient la clé publique du serveur Web qui souhaite réaliser du https. Le navigateur chiffre avec cette clé publique APRÈS avoir contrôlé le certificat.

Les certificats numériques

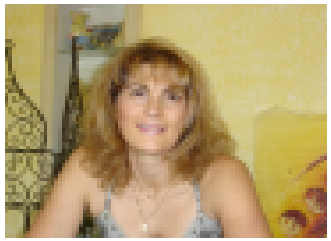


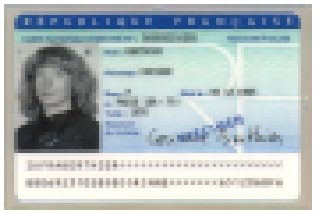
Création de la signature numérique

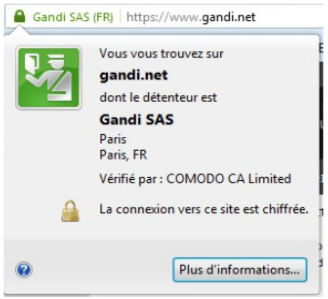


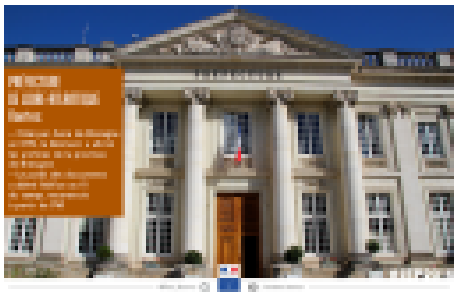
Vérification de la signature numérique

Châine de confiance









Stuxnet

- Stuxnet est un ver informatique supposé développé conjointement par les États-Unis et Israël pour s'attaquer à des systèmes iraniens.

Stuxnet

- Stuxnet est un ver informatique supposé développé conjointement par les États-Unis et Israël pour s'attaquer à des systèmes iraniens.
- C'est le premier ver découvert qui espionne et reprogramme des systèmes industriels, ce qui comporte un risque élevé.

Stuxnet

- Stuxnet est un ver informatique supposé développé conjointement par les États-Unis et Israël pour s'attaquer à des systèmes iraniens.
- C'est le premier ver découvert qui espionne et reprogramme des systèmes industriels, ce qui comporte un risque élevé.
- Il cible spécifiquement les systèmes SCADA utilisés pour le contrôle commande de procédés industriels.

Stuxnet

- L'étude du ver fait encore apparaître que deux certificats ont été volés à JMicron et Realtek.

Stuxnet

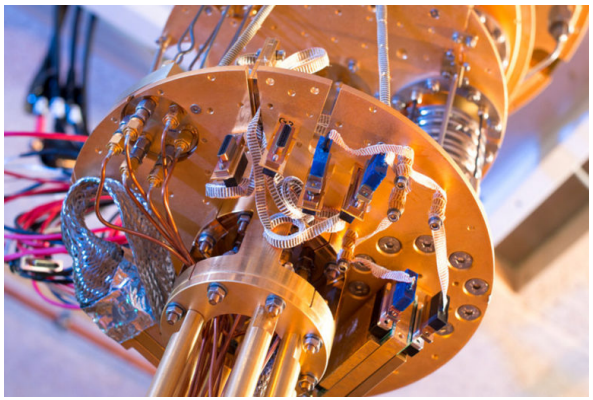
- L'étude du ver fait encore apparaître que deux certificats ont été volés à JMicron et Realtek.
- Le système vérifie en effet l'authenticité des codes exécutables auprès d'une autorité de certification : Verisign.
  Mais le code exécutable modifié disposait des certificats originaux et l'autorité de certification les reconnaissait comme valides !

Stuxnet

- L'étude du ver fait encore apparaître que deux certificats ont été volés à JMicron et Realtek.
- Le système vérifie en effet l'authenticité des codes exécutables auprès d'une autorité de certification : Verisign.
  Mais le code exécutable modifié disposait des certificats originaux et l'autorité de certification les reconnaissait comme valides !
- Comment les certificats ont-ils été volés ? Infiltration, commandos, espionnage, achat de personnes...

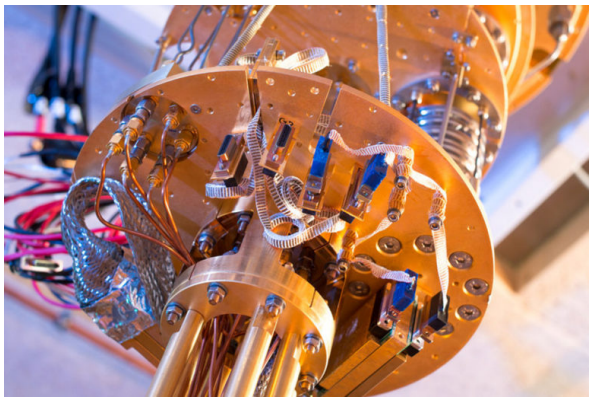
La fin du chiffrement ?

Un ordinateur quantique casse le chiffrement RSA sur 2048 bits en 8 heures (4 Juin 2019)



La fin du chiffrement ?

Un ordinateur quantique casse le chiffrement RSA sur 2048 bits en 8 heures (4 Juin 2019)



Prix d'un ordinateur quantique

15 Millions de dollars