

Architecture PKI & Bitcoins

Pascal Lafourcade

*Chaire industrielle,
Confiance numérique*



AuDACES 2016

Applications



Clef symétrique



Exemples

- ▶ DES
- ▶ AES

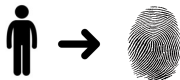
Chiffrement à clef publique



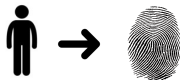
Exemples

- ▶ RSA : $c = m^e \pmod n$
- ▶ ElGamal : $c \equiv (g^r, h^r \cdot m)$

Fonction de Hachage (SHA-1, SHA-3)



Fonction de Hachage (SHA-1, SHA-3)

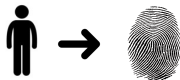


Propriétés de résistance

► Pré-image



Fonction de Hachage (SHA-1, SHA-3)

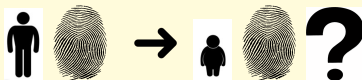


Propriétés de résistance

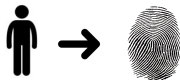
- ▶ Pré-image



- ▶ Seconde Pré-image



Fonction de Hachage (SHA-1, SHA-3)

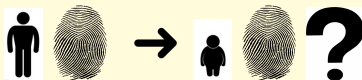


Propriétés de résistance

- ▶ Pré-image



- ▶ Seconde Pré-image



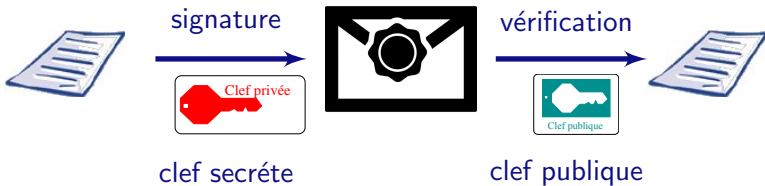
- ▶ Collision



Signature



Signature



RSA: $m^d \pmod n$

Plan

Sécuriser vos emails

Plan

Sécuriser vos emails

Bitcoins

Plan

Sécuriser vos emails

Bitcoins

Conclusion

Plan

Sécuriser vos emails

Bitcoins

Conclusion

Octobre 2014



L'importance de la vie privée
Why privacy matters?

Par Glenn Greenwald

Les gens pensent ne rien avoir à cacher ...



<http://jenairienacacher.fr/>

La sécurité des emails par défaut



Pretty Good Privacy

Logiciel de chiffrement, déchiffrement, signature de courriers électroniques, inventé par Phil Zimmermann en 1991.

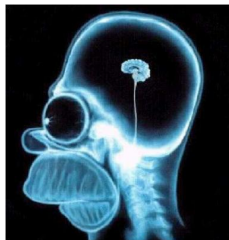


*Si la vie privée est mise hors la loi,
seuls les hors-la-loi auront une vie privée.*

If privacy is outlawed, only outlaws will have privacy

Est-ce si difficile ?

1. Télécharger l'outil GPG et l'installer.
2. Générer une paire de clefs ≥ 4096 bits
3. Importer votre clefs
4. Télécharger les clefs de vos amis
5. Envoyer des emails chiffrés et/ou signés.



Plan

Sécuriser vos emails

Bitcoins

Conclusion

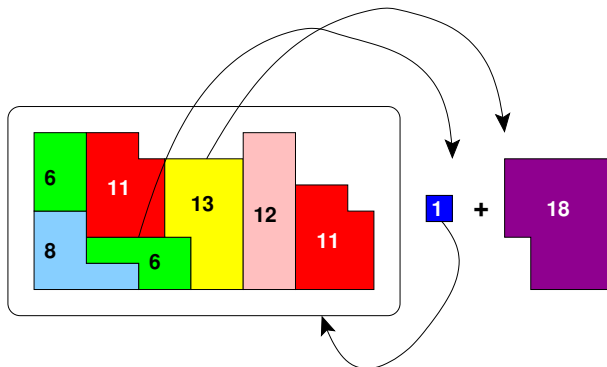
Bitcoin : monnaie électronique

Créée en 2008 par Satoshi Nakamoto (1 BTC \approx 405 euros)



1	BTC = 1 Bitcoin	
0,01	BTC = 1 cBTC	= 1 centiBitcoin (ou bitcent)
0,001	BTC = 1 mBTC	= 1 milliBitcoin
0,000 001	BTC = 1 μ BTC	= 1 microBitcoin
0,000 000 01	BTC = 1 Satoshi	

Payer avec des bitcoins 18 BTC



Miner des Bitcoins



Miner des Bitcoins



Les “*mineurs*” valident les transactions contre des bitcoins



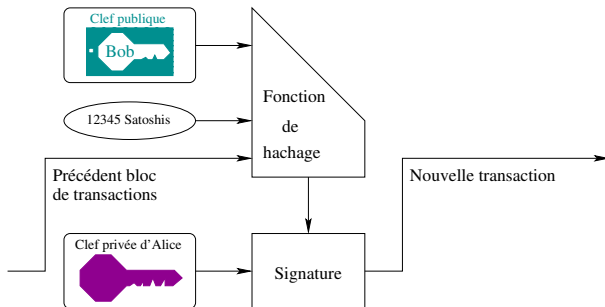
Miner des Bitcoins

- ▶ Valider = résoudre un **objectif de hachage**
- ▶ Récompense initiale 50 BTC pour une validation
- ▶ Divisée par 2 tous les 210000 validations

$$\sum_{i=0}^{32} \frac{50}{2^i} \times 210\,000 = 21 \text{ millions BTC}$$

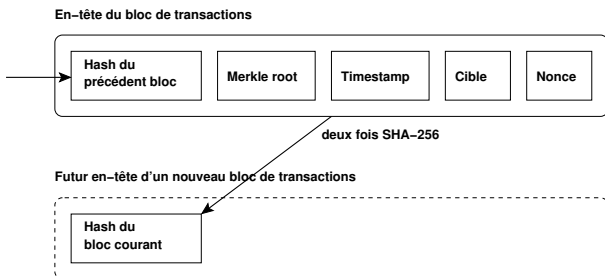
Bitcoins : Fonctionnement

Alice donne 12345 Satoshis ($\approx 5c$) à Bob.



- ▶ Seuls des bitcoins possédés peuvent être dépensés

Bitcoins : Objectif de hachage (Proof of work)



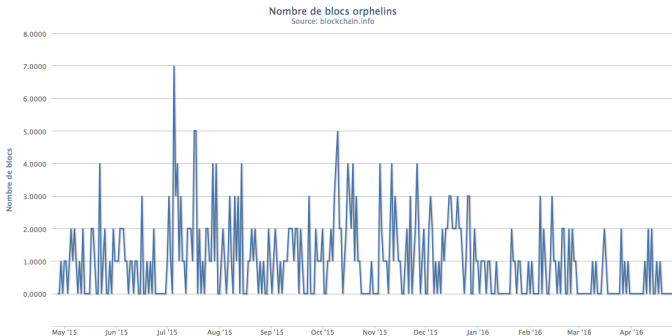
Avoir un zéro de plus au début
SHA-256(SHA-256(en-tête de bloc))

- ▶ les transactions passées (65 Go)
- ▶ les transactions à valider
- ▶ les secondes depuis 01/01/1970
- ▶ un nonce
- ▶ etc ...

Bitcoins : Validation des transactions

00000000000000000254845fa930deac4086b3e3bce21147e93f463b206d8076

- ▶ Validation toutes les 10 minutes (6 confirmations)
- ▶ La chaîne la plus longue persiste (attaque 51 %)



Autres crypto-monnaies > 112



Chaîne de Cunningham

$1 \leq i < n, p_{i+1} = ap_i + b$ pour des premiers entre eux fixés a, b

Séminaire Confiance numérique

Jordi Herrera, Universitat Autònoma de Barcelona (UAB)



Is bitcoin a suitable research topic?

<http://confiance-numerique.clermont-universite.fr>

Plan

Sécuriser vos emails

Bitcoins

Conclusion

Rappels

Choses à retenir

- ▶ La sécurité est omni-présente
- ▶ Devenir acteur de votre sécurité
- ▶ Chiffrer et signer vos emails
- ▶ Bitcoins

Merci pour votre attention.

Questions ?

**Architectures PKI
et
communications
sécurisées**

Master • Écoles d'ingénieurs



Jean-Guillaume Dumas
Pascal Lafourcade
Patrick Redon

Préface de Guillaume Poupard

DUNOD