La procédure expertale

DES DOCUMENTS ET DES HOMMES

authentifier les uns et identifier les autres

19 janvier 2011

CNEJITA

Code civil

Art 1316-3

L’écrit sur support électronique a la même force probante que l ’écrit sur support papier

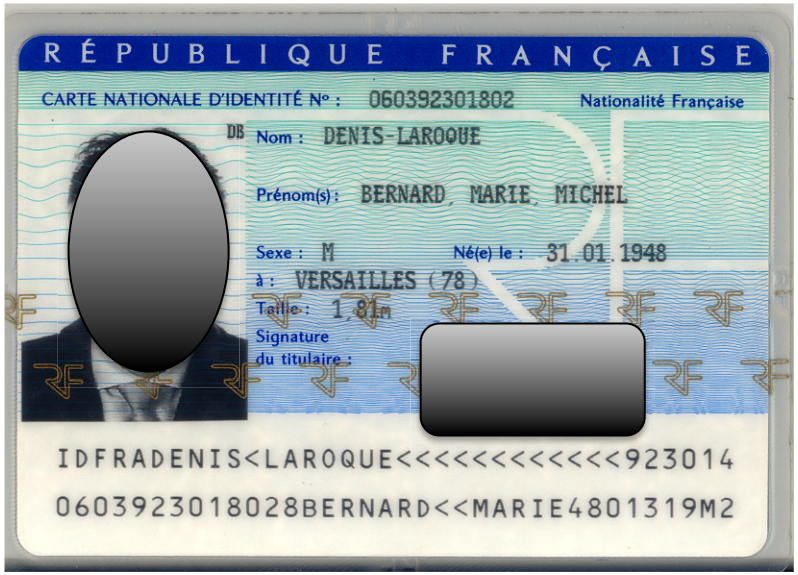
Code de procédure civile

Art 748-2

Le destinataire des envois, remises et notifications mentionnés à l'article 748-1 doit consentir expressément à l'utilisation de la voie électronique, à moins que des dispositions spéciales n'imposent l'usage de ce mode de communication.

CNEJITA

Identification et authentification



La Sécurité électronique : la cryptographie asymétrique

CNEJITA

Exemple

$$17\ 159 \times 10\ 247 = 175\ 828\ 273$$

CNEJITA

Autre exemple

408 508 091= ?

408 508 091 (suite)

/ 2 reste : 1
/ 3 reste : 2
/ 5 reste : 1
/ 7 reste : 5
/ 11 reste : 2
/ 13 reste : 4
/ 17 reste : 12
/ 19 reste : 16
/ 23 reste : 8
/ 29 reste : 26
/ 31 reste : 11
/ 37 reste : 8
/ 41 reste : 40
/ 43 reste : 7
/ 47 reste : 24
/ 53 reste : 44
/ 59 reste : 56
/ 61 reste : 58
/ 67 reste : 46
/ 71 reste : 6
/ 73 reste : 18

/ 79 reste : 39
/ 83 reste : 19
/ 89 reste : 49
/ 97 reste : 60
/ 101 reste : 57
/ 103 reste : 100
/ 107 reste : 67
/ 109 reste : 71
/ 113 reste : 96
/ 127 reste : 18
/ 131 reste : 49
/ 137 reste : 121
/ 139 reste : 18
/ 149 reste : 6
/ 151 reste : 90
/ 157 reste : 57
/ 163 reste : 99
/ 167 reste : 39
/ 173 reste : 77
/ 179 reste : 19
/ 181 reste : 141

Etc...

408 508 091 (suite)

Etc...

...

```
/18  313 reste :  0
```

408 508 091 / 18 313 = 22 307

18 313 est un nombre de 15 bits. Sa recherche a nécessité 2000 divisions

Connaissant 18 313, on a trouvé 22307 en une division

CNEJITA

L ’asymétrie

- Pour un nombre de 2000 bits (facteurs de 1000 bits) il faut 10^{298} divisions
- Décomposer en facteurs premiers d ’environ 1000 bits un nombre de 2000 bits est virtuellement impossible.

CNEJITA

Les fonctions asymétriques

- Il existe une fonction mathématique F et des paires d'entiers naturels (A,A') tels que,
  - ∀M, F[F(M,A),A']=M
  - Et il n'est pas possible de calculer M à partir de F(M,A) si on ne connaît pas A'

CNEJITA

Le cryptage RSA

- On fabrique un nombre N = p x q (p et q premiers)
- On choisit un nombre e premier avec (p-1)(q-1)
- On calcule d tel que ed = 1 + k(p-1)(q-1)

  Théorème de Bezout : si c est le pgcd de a et b, alors il existe deux entiers relatifs u et v tels que c = au + bv)

  Algorithme d'Euclide étendu permet de calculer u et v
- On détruit p et q
  - (e,N) est la clé publique et (N, d) la clé privée
- Signature $C \equiv M^d \pmod N$
- Vérification $M \equiv C^e \pmod N$

CNEJITA

Exemple d'algorithme d'Euclide

p = 19 ; q = 37 ; N = pq = 703 ; (p-1)(q-1) = 648 ; e = 157

- 648 = 4 x157 + 20
- 157 = 7x20 + 17
- 20 = 1x17 + 3
- 17 = 5x3 + 2
- 3 = 1x2 + 1

55
-7
6
-1

55x648 = 227x157 +1

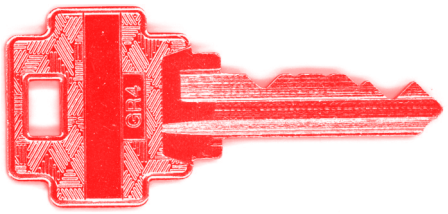
-7x157= -55x20 + 1

6 x20 = 7 x 17 + 1

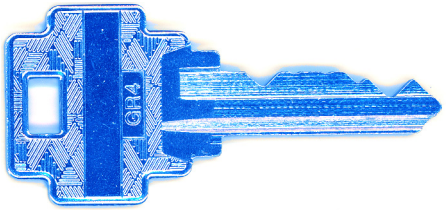
-17 = -6x3 + 1

$\Rightarrow$ d = -227

Un “Bi-clés”



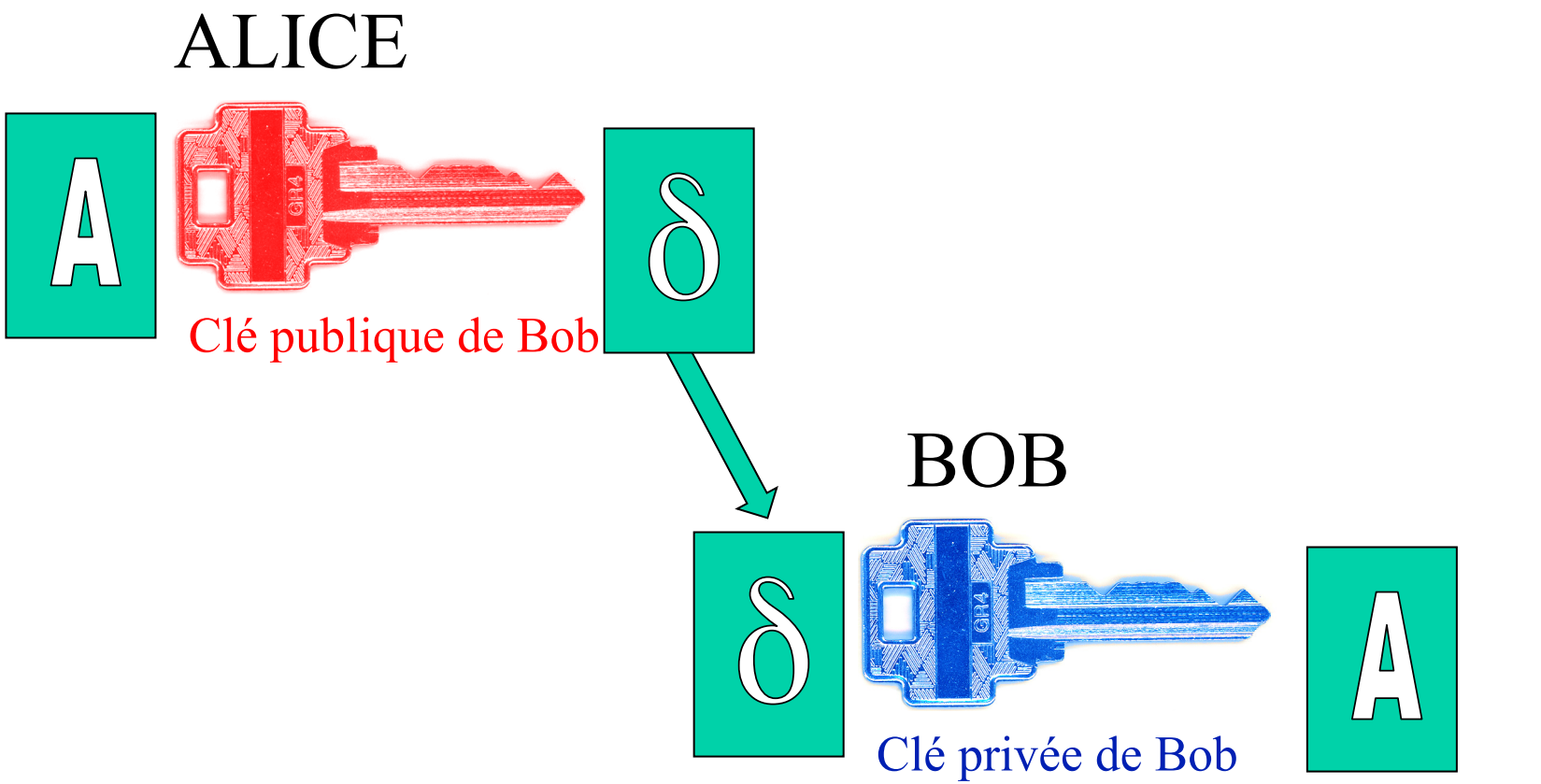
Clé publique : peut être copiée et communiquée sans danger



Clé privée : reste toujours cachée chez son propriétaire

CNEJITA

Cryptage



Fonctions de hachage asymétriques

- Un message M de longueur quelconque
- Résultat h = H(M) de longueur m donnée
- Impossible de fabriquer un M à partir d ’un h donné
- Impossible de fabriquer M et M’ tels que

H(M) = H(M’)

CNEJITA

Fonctions de hachage asymétriques

- MD5 (Message Digest 5) 128 bits
- SHA1 (Secure Hash Algorithm) 160 bits

CNEJITA

La signature électronique

=

Cryptage d’un hachis à l’aide de la clé privée du signataire

Alice signe son message

Lorem ipsum dolor sic amet

21 3A BB C4 FF

Empreinte digitale

6B 77 3A CF 2D

Signature

CNEJITA

Bob le reçoit

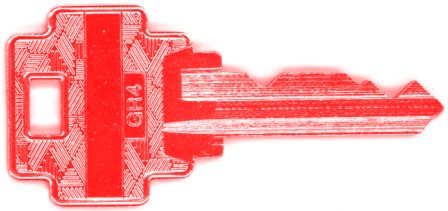
Lorem ipsum dolor sic amet

6B 77 3A CF 2D

Signature

21 3A BB C4 FF

Empreinte digitale



21 3A BB C4 FF

CNEJITA

La Sécurité électronique

- Identification : celui ou celle qui possède la clé privée d'Alice est forcément Alice
- Authentification : l'autorité de certification certifie qu'elle a délivré cette clé publique à Alice

ou

- Bob connais bien Alice et elle lui a remis elle-même sa clé publique

Problématique

- Authentification de la signature
  - Usurpation d ’identité
- Intégrité du document signé
  - Falsification du contenu du document signé
- Non répudiation par le signataire
  - Refus du signataire de reconnaître sa signature

CNEJITA

Horodatage

- Un tiers horodateur possède une horloge très précise. Il crée un

  « jeton d'horodatage »

  qui est une signature d'un hash du document accompagné de la date et l'heure.

- Garantit l'intégrité du document, même non signé.

Opalexe

- Ne nécessite pas de signature (l'authentification se fait à l'entrée)
- Seuls les outputs (rapport) doivent être signés

CNEJITA

Les communications

- Les dires à expert, les notes aux parties ou le rapport sont des écrits. Bien des pièces aussi.

- Mais on peut communiquer des pièces qui ne sont pas des écrits (enregistrements audio, séquences vidéo, feuilles de calcul etc…)

Les écrits

L'écrit électronique doit au moins respecter les exigences du code civil, et notamment (art 1316-1)

« qu'il soit établi et conservé dans des conditions de nature à en garantir l'intégrité »

- Le document doit être le même quel que soit la personne qui l'ouvre : pagination, date, hiérarchisation des titres, polices de caractères etc...

CNEJITA

Les formats d'écrit

« qu'il soit établi et conservé dans des conditions de nature à en garantir l'intégrité »

- Un format d'image
  - tiff
  - jpeg
  - bmp
  - Adobe pdf, Compuserve gif, Adobe ps

- Une norme mondiale : le pdf(a)

Les formats d'écrit

« qu'il soit établi et conservé dans des conditions de nature à en garantir l'intégrité »

- Par définition, ne JAMAIS considérer comme des écrits électroniques les documents au format de traitement de texte (Word), de calcul (Excel), de dessin (Photoshop, Illustrator, Autocad etc.)

CNEJITA

Un exemple : MS Word

Le 10 décembre 2010

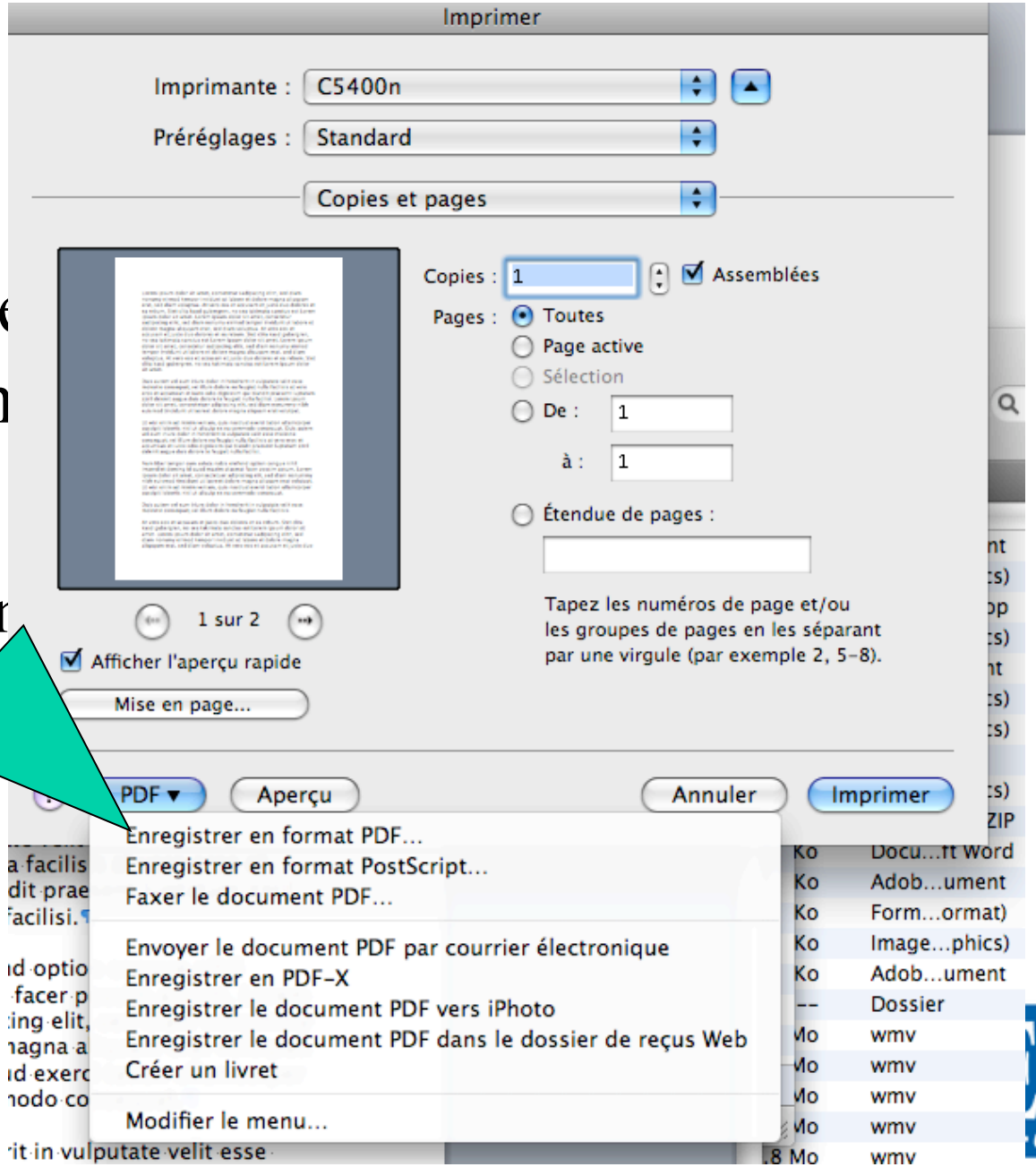
Voir page 41

Le 15 décembre 2010

Voir page 41
(mais ce n'est plus page 41)

CNEJITA

- Les docume
  voulez com
  - – figer
  - – Directe



Les documents

- Les documents papier sont scannés en pdf

Vous ne perdrez jamais votre temps
en scannant

Merci de votre attention