La signature électronique

Dou Henri
douhenri@yahoo.fr

Mars 2019

Il faudra attendre 1999 pour qu'en Europe les **signatures électroniques**soient officiellement reconnues par la loi, avec la mise en place de la directive 1999/93/CE. Elles prennent alors la même valeur qu'une signature manuscrite lors d'un accord entre deux parties. En France, la loi n° 2000-230 parue le 13 mars 2000 et son décret n° 2001-272 du 30 mars 2001viennent officialiser l'usage de la signature électronique dans notre pays.

Des organismes spécialisés sont alors créés pour délivrer des **certificats numériques** validant l'authenticité des diverses signatures électroniques. Ces certificats sont comme une carte d'identité contenant toutes les informations privées et publiques nécessaires à l'émission d'une signature électronique. Un problème se pose cependant : chaque pays gère ses certificats électroniques à sa façon. Heureusement, dès le 1er juillet 2016, un nouveau règlement européen vient clarifier les choses, permettant d'homogénéiser les diverses normes de signature électronique au sein de l'Union européenne. La gestion des documents dans l'UE se voit donc simplifiée. En revanche, il n'en va pas de même pour les pays hors-UE.

Pour terminer cette partie sur la législation, une petite précision s'impose : la **signature numérique** ne doit pas être confondue avec la signature numérisée faite par exemple avec un stylet sur une tablette. Bien que cette dernière soit aussi reconnue légalement depuis 2010, elle n'est pas l'objet de cet article.

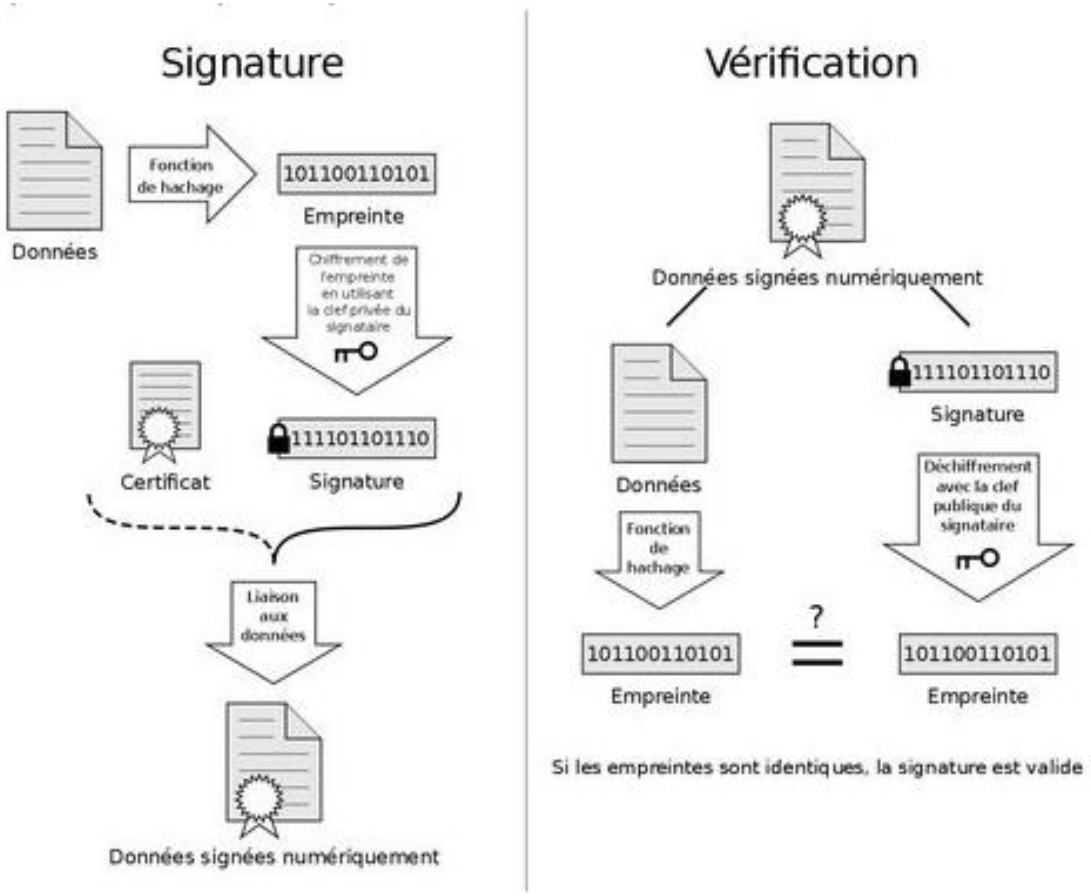
https://www.clubic.com/antivirus-securite-informatique/article-837828-1-signature-electronique-comment.html

Nous prendrons pour cet exemple le cas d'une entreprise **Alice** qui envoie un contrat au format PDF à une entreprise **Bob** Pour procéder, le logiciel de l'entreprise Alice va créer un *hachage* du contrat. Cette méthode consiste à générer une empreinte composée de chiffres et de lettres propre au document. La moindre modification dudit document entraine alors une modification du hachage. Vous avez d'ailleurs probablement déjà vu les sigles *MDA* ou *SHA-1*. Ce sont des protocoles de hachage, destinés à vérifier l'intégrité de données.

Une fois le *hash* - le mot anglais pour hachage - réalisé, il est associé à deux clés données par le **certificat numérique** : une privée et une publique. La clé privée va chiffrer (on évite l'anglicisme *« crypter »*) le hash, ce qui donne la fameuse signature électronique. Le tout est ensuite envoyé au destinataire avec la clé publique. Cette dernière est connue de nos deux entreprises.

Lors de la réception du contrat, l'entreprise Bob va déchiffrer le hachage du contrat avec la clé publique. Une fois déchiffré, le hash est recalculé par le logiciel de l'entreprise Bob. S'il est identique à l'original, alors le destinataire sera averti de son authenticité et obtiendra l'identité du signataire. Bien évidemment, si le hachage ne colle pas, alors le destinataire saura que le document a été modifié avant sa réception.

https://www.clubic.com/antivirus-securite-informatique/article-837828-1-signature-electronique-comment.html



Présentation issue de Wikipedia

Le coût de la signature électronique

Dousign 9 € mois
Eversign 9,99 € mois 5 documents gratuits par mois
Yousign Tarif sur mesure
Adobe sign 11,99 € mois
SignEasy pas d'indication
Secure signing 9,95 € mois 3 documents gratuits par mois
Universign Tarif sur mesure
eSign Live 20 $ US mois (déploiement possible sur Clouds privé ou public)

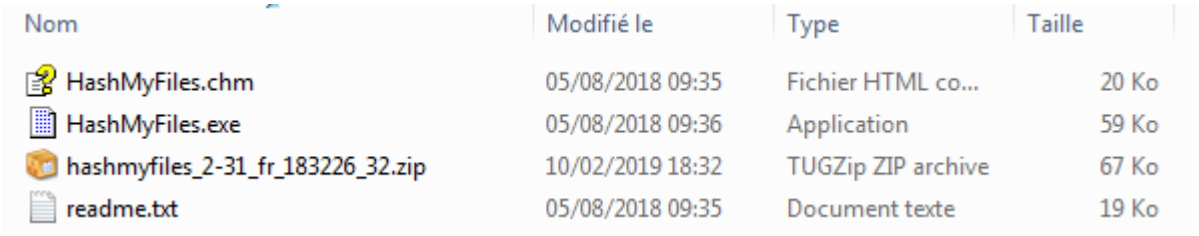
Le coût d'un logiciel de cryptage

Gratuit

Il existe d'autres logiciels gratuits
Mais aussi de nombreuses offres payantes

Le Hash code ou empreinte d’un fichier

HashMyFiles



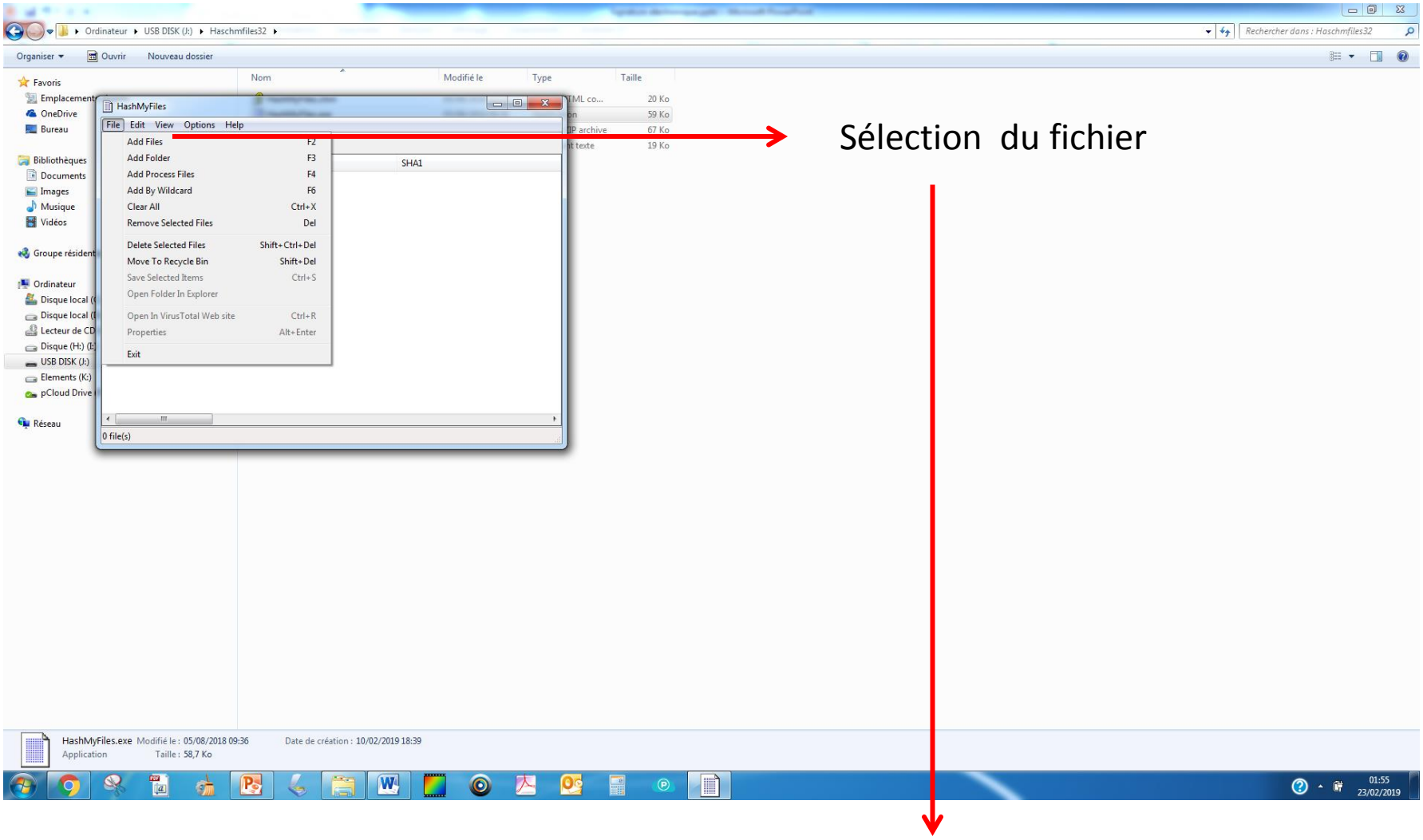
Nom	Modifié le	Type	Taille
HashMyFiles.chm	05/08/2018 09:35	Fichier HTML co...	20 Ko
HashMyFiles.exe	05/08/2018 09:36	Application	59 Ko
hashmyfiles_2-31_fr_183226_32.zip	10/02/2019 18:32	TUGZip ZIP archive	67 Ko
readme.txt	05/08/2018 09:35	Document texte	19 Ko

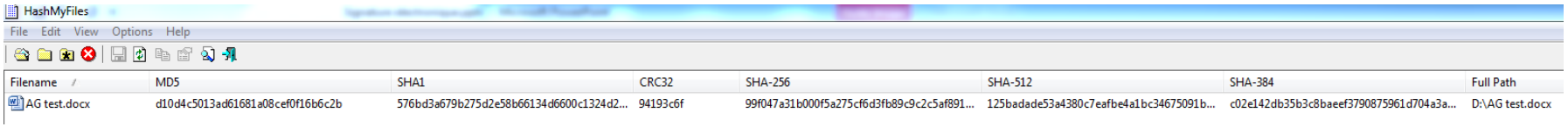
Autres application plus puissante

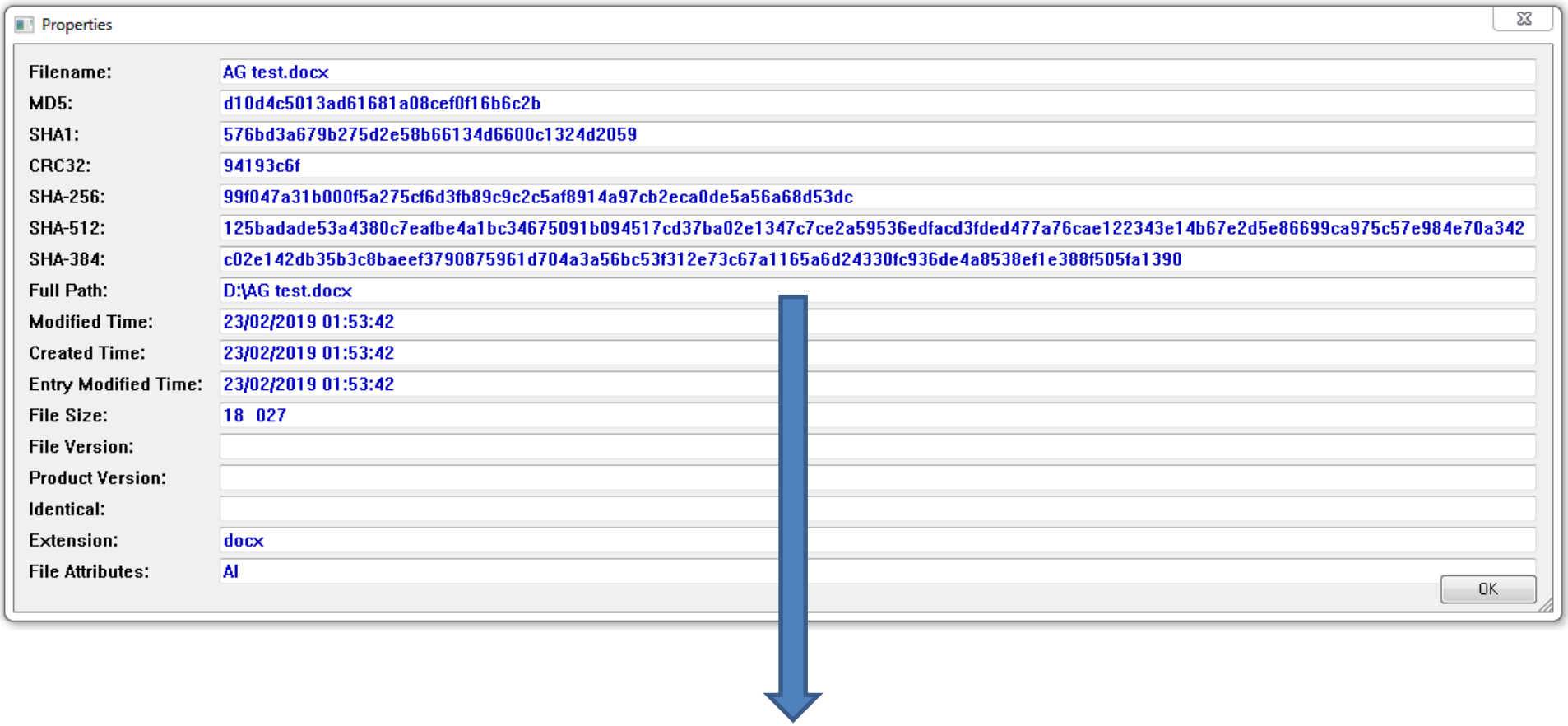
Lors de l’assemblée générale de notre association la majorité des membres ont été d’accord pour adopter les apports de capitaux de nouveaux actionnaires. Cependant une courte majorité s’est prononcée pour ne pas adopter la proposition de l’actionnaire ABCD. Cette proposition a fait l’objet d’un compte rendu qui sera transmise à notre avocat.
Corte le 12 Janvier 2019

Sauvé sous le nom AG test.docx

Nous allons calculer son empreinte


HashMyFiles
File Edit View Options Help
Add Files F2
Add Folder F3
Add Process Files F4
Add By Wildcard F6
Clear All Ctrl+X
Remove Selected Files Del
Delete Selected Files Shift+Ctrl+Del
Move To Recycle Bin Shift+Del
Save Selected Items Ctrl+S
Open Folder In Explorer
Open In VirusTotal Web site Ctrl+R
Properties Alt+Enter
Exit
SHA1
0 file(s)
Sélection du fichier


HashMyFiles
File Edit View Options Help
Filename
MD5
SHA1
CRC32
SHA-256
SHA-512
SHA-384
Full Path
AG test.docx
d10d4c5013ad61681a08cef0f16b6c2b
576bd3a679b275d2e58b66134d6600c1324d2...
94193c6f
99f047a31b000f5a275cf6d3fb89c9c2c5af891...
125badade53a4380c7eafbe4a1bc34675091b...
c02e142db35b3c8baeef3790875961d704a3a...
D:\AG test.docx



Les différentes empreintes calculées avec des systèmes différents

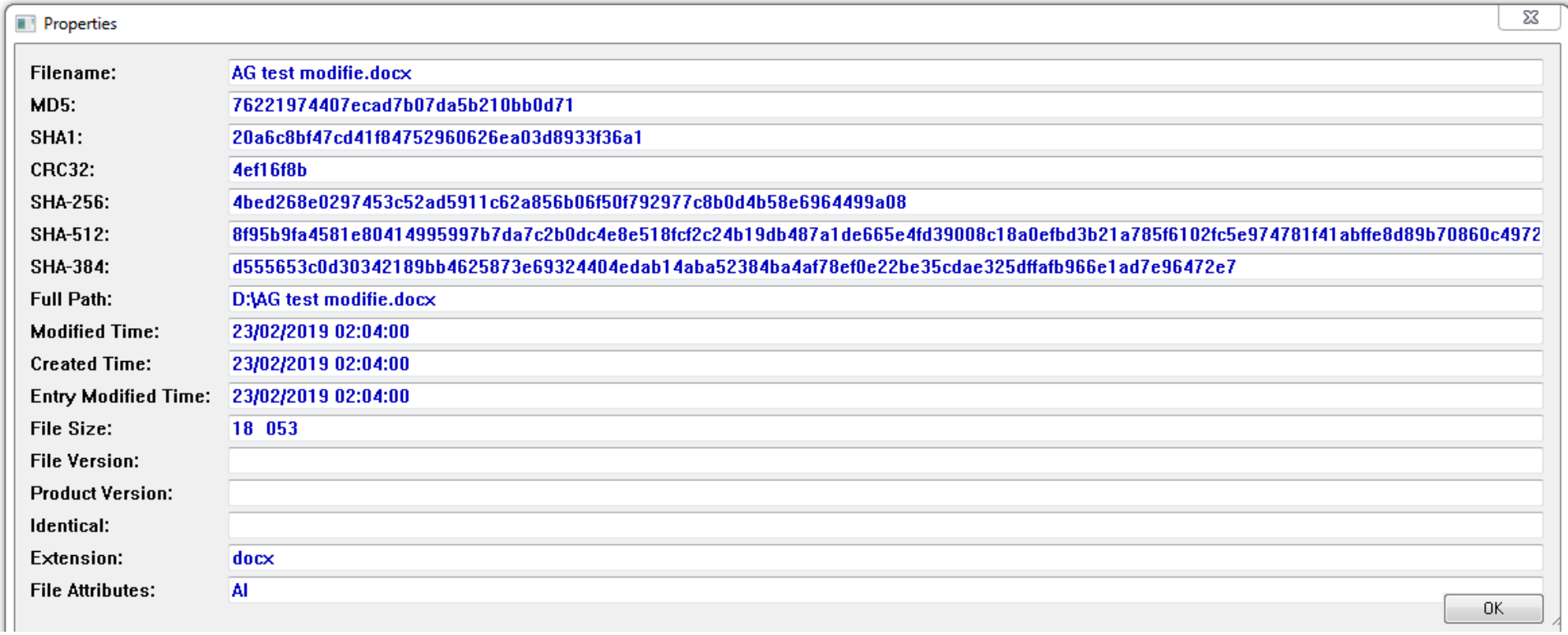
On prend la photographie avec un téléphone portable

Lors de l’assemblée générale de notre association la majorité des membres ont été d’accord pour adopter les apports de capitaux de nouveaux actionnaires. Cependant une courte majorité s’est prononcée pour **ne pas** adopter la proposition de l’actionnaire ABCD. Cette proposition a fait l’objet d’un compte rendu qui sera transmise à notre avocat.
Corte le 12 Janvier 2019

On enlève ne pas

Sauvé sous le nom AG test modifié.docx

Nous allons calculer son empreinte


Properties
Filename:
AG test modifie.docx
MD5:
76221974407ecad7b07da5b210bb0d71
SHA1:
20a6c8bf47cd41f84752960626ea03d8933f36a1
CRC32:
4ef16f8b
SHA-256:
4bed268e0297453c52ad5911c62a856b06f50f792977c8b0d4b58e6964499a08
SHA-512:
8f95b9fa4581e80414995997b7da7c2b0dc4e8e518fcf2c24b19db487a1de665e4fd39008c18a0efbd3b21a785f6102fc5e974781f41abffe8d89b70860c4972
SHA-384:
d555653c0d30342189bb4625873e69324404edab14aba52384ba4af78ef0e22be35cdae325dffafb966e1ad7e96472e7
Full Path:
D:\AG test modifie.docx
Modified Time:
23/02/2019 02:04:00
Created Time:
23/02/2019 02:04:00
Entry Modified Time:
23/02/2019 02:04:00
File Size:
18 053
File Version:
Product Version:
Identical:
Extension:
docx
File Attributes:
AI
OK

On compare les deux empreintes

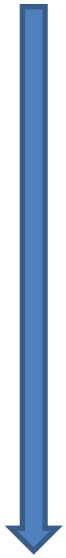
Filename:	AG test.docx
MD5:	d10d4c5013ad61681a08cef0f16b6c2b
SHA1:	576bd3a679b275d2e58b66134d6600c1324d2059
CRC32:	94193c6f
SHA-256:	99f047a31b000f5a275cf6d3fb89c9c2c5af8914a97cb2eca0de5a56a68d53dc
SHA-512:	125badade53a4380c7eafbe4a1bc34675091b094517cd37ba02e1347c7ce2a59536edfacd3fded477a76cae122343e14b67e2d5e86699ca975c57e984e70a342
SHA-384:	c02e142db35b3c8baeef3790875961d704a3a56bc53f312e73c67a1165a6d24330fc936de4a8538ef1e388f505fa1390

Fichier original

Filename:	AG test modifie.docx
MD5:	76221974407ecad7b07da5b210bb0d71
SHA1:	20a6c8bf47cd41f84752960626ea03d8933f36a1
CRC32:	4ef16f8b
SHA-256:	4bed268e0297453c52ad5911c62a856b06f50f792977c8b0d4b58e6964499a08
SHA-512:	8f95b9fa4581e80414995997b7da7c2b0dc4e8e518fcf2c24b19db487a1de665e4fd39008c18a0efbd3b21a785f6102fc5e974781f41abffe8d89b70860c4972
SHA-384:	d555653c0d30342189bb4625873e69324404edab14aba52384ba4af78ef0e22be35cdae325dffafb966e1ad7e96472e7

Fichier modifié

Envoi du fichier et sécurité



Le fichier original est envoyé par email

Les hash codes originaux sont envoyés soit via un email différent (non recommandé) ou par la poste ou par fax, **plus généralement via un MMS** (recommandé)

Le programme de hash code utilisé est le même pour la personne qui reçoit le fichier

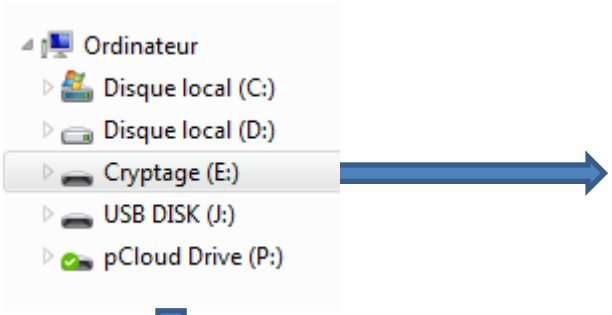
Elle calcule l'empreinte

Elle effectue la comparaison

Si le hash code calculé par la personne qui reçoit le message est le même que l'original, cela veut dire que le fichier n'a pas été modifié.

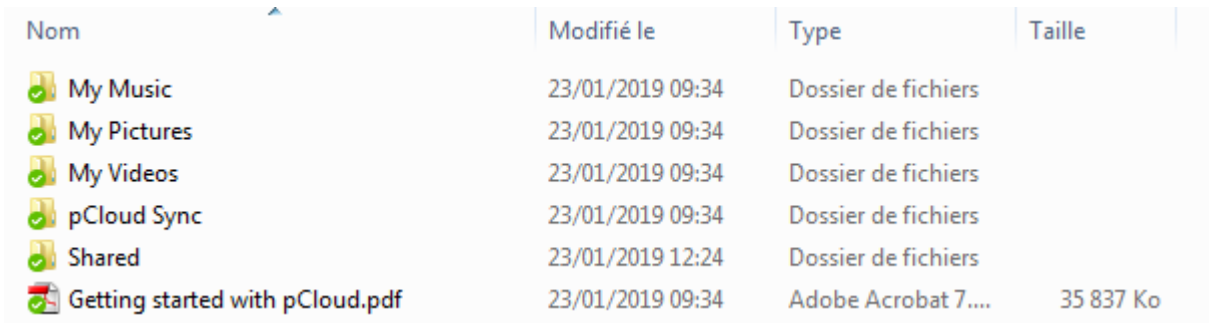
Logiciel de cryptage: cryptainer LE (gratuit)

Une fois le logiciel installé

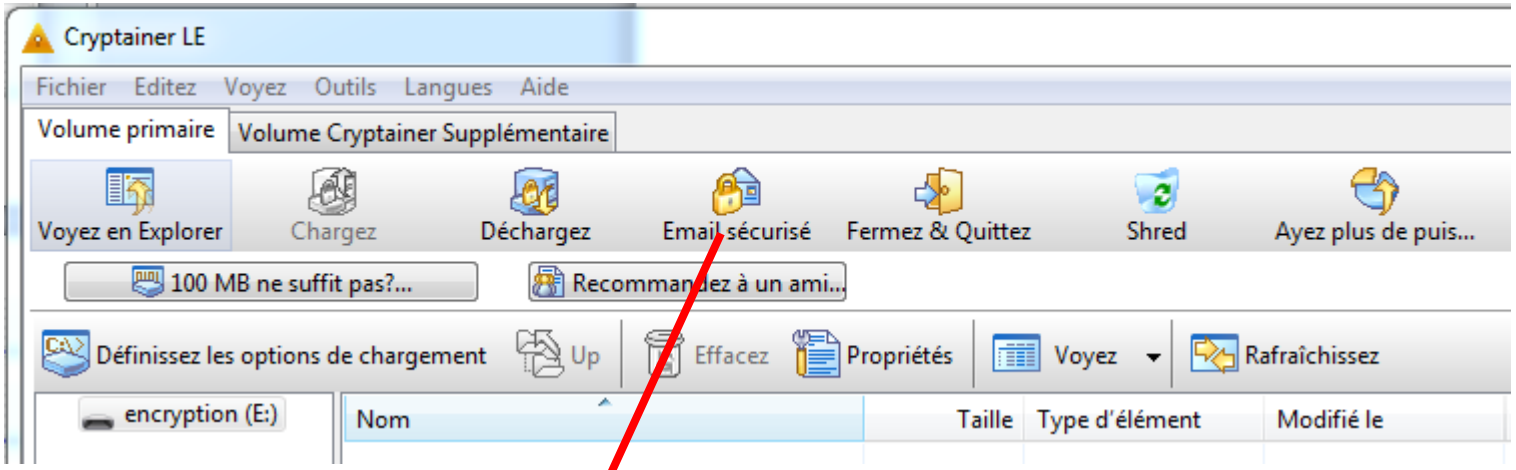


Au cours de l'installation création d'un volume où seront placés les textes cryptés

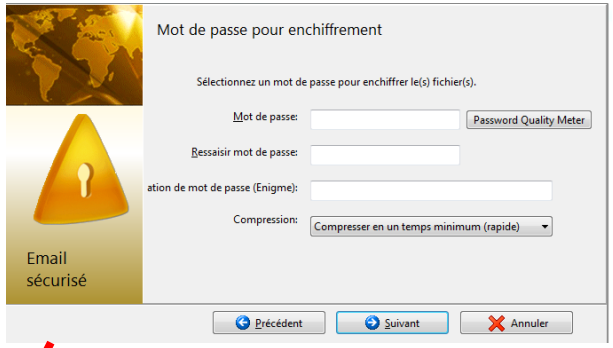
Remarquer la présence d'un Cloud virtuel.

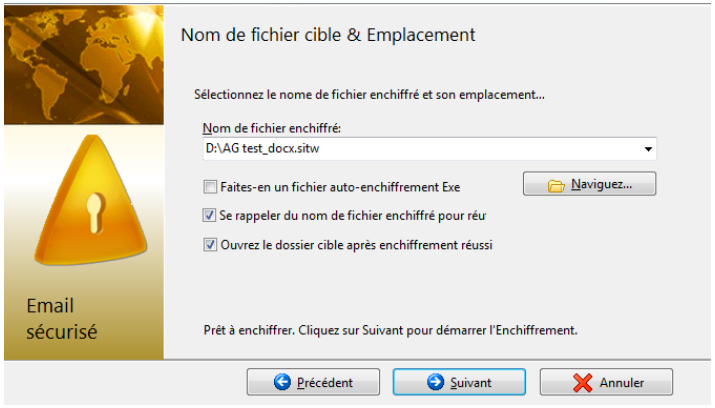


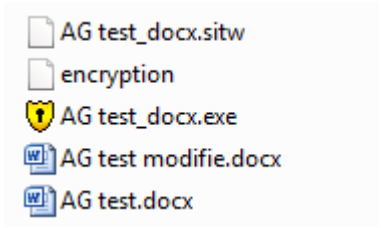
Cryptainer



Choix du fichier à enchiffrer
Deux méthodes
Self extracting (.exe)





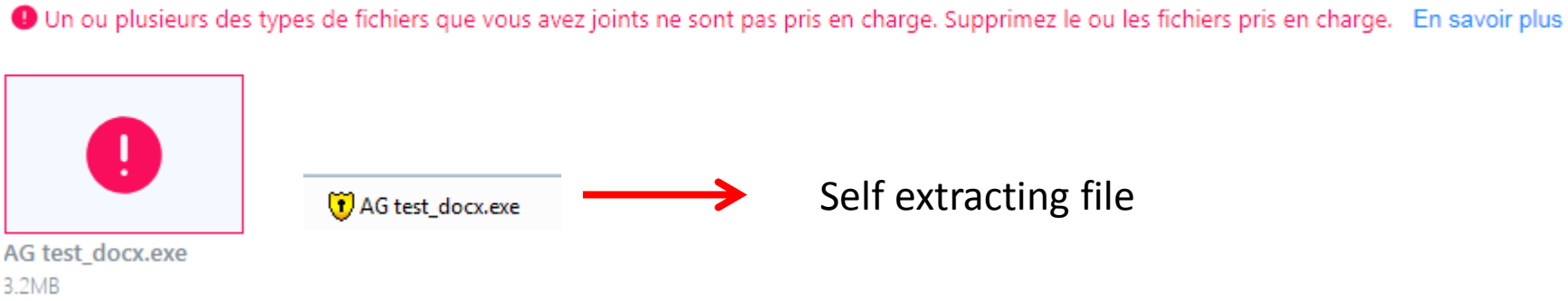


Envoi de fichiers cryptés par e-mail

Envoi par mail réussi

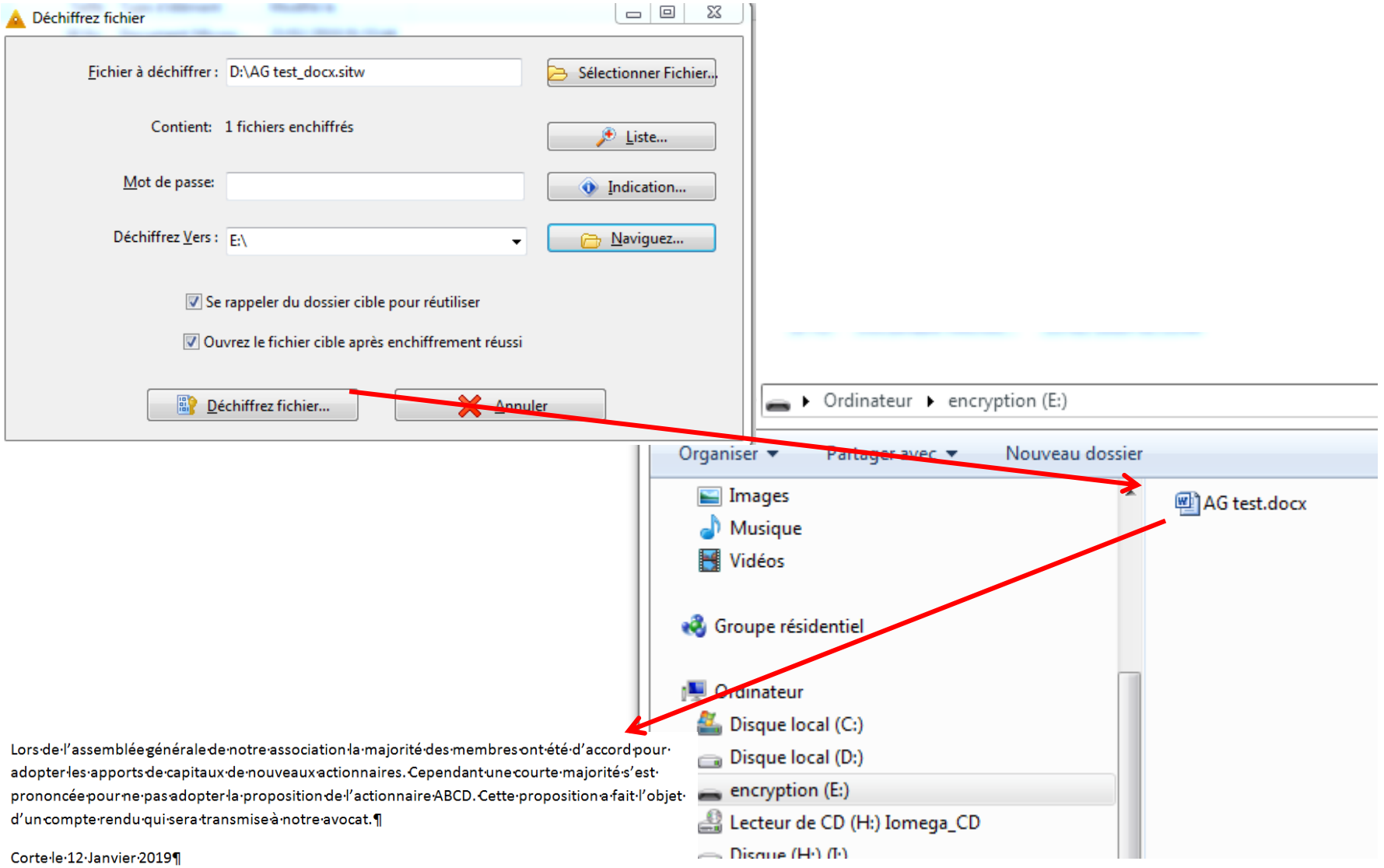
Mot de passe utilisé pour l'encryption et l'ouverture du fichier:
dupascalpaoli

Envoi du fichier crypté avec yahoo mail:



Self extracting file

Déchiffrement



Lors·de·l'assemblée·générale·de·notre·association·la·majorité·des·membres·ont·été·d'accord·pour·adopter·les·apports·de·capitaux·de·nouveaux·actionnaires.·Cependant·une·courte·majorité·s'est·prononcée·pour·ne·pas·adopter·la·proposition·de·l'actionnaire·ABCD.·Cette·proposition·a·fait·l'objet·d'un·compte·rendu·qui·sera·transmise·à·notre·avocat.¶

Corte·le·12·Janvier·2019¶

Le déchiffrement nécessite pour le correspondant d'avoir le même logiciel pour décrypter.

Noter que yahoo mail ne permet pas l'envoi du fichier en exe autoextractible.

Que faire ? → Changer le nom du fichier !

Ensuite votre correspondant change le nom à nouveau et décrypte le fichier avec le mot de passe.

Dans le futur (on peut estimer à 10 ans)

Les ordinateurs quantiques qui travaillerons à une vitesse sans commune mesure avec les ordinateurs actuels, permettront de « casser » tous les codes.

Comment fonctionne un ordinateur quantique:
https://www.futura-sciences.com/sciences/definitions/physique-ordinateur-quantique-4348/

La technologie quantique est ce que l'on nomme une **« technologie disruptive »**
En effet elle rend caduque la Loi de Moore.

https://www.latribune.fr/opinions/qui-gagnera-la-bataille-de-l-ordinateur-quantique-786053.html
Qubit or not qubit ? Telle est la question à l'âge de l'informatique quantique. Cette technologie pourrait résoudre des problèmes que même les ordinateurs les plus puissants ne savent pas résoudre. Son potentiel de disruption est gigantesque, à condition que cela marche. La Chine a annoncé le 3 mai 2017 que des chercheurs de Shanghai avaient mis au point le premier ordinateur quantique dépassant un ordinateur classique. (Crédits : Capture : News.cn)

https://www.lesechos.fr/17/08/2016/LesEchos/22256-071-ECH_satellites---pekin-lance-le-premier-satellite-inviolable.htm?texte=quantique%20chine
La Chine lance le premier satellite à communication quantique

Merci pour votre attention