

LA CRYPTOGRAPHIE





DEFINITIONS

DEFINITIONS

CRYPTOLOGIE :

La cryptologie est la science du secret. Elle a pour objet les écrits secrets et leur étude. Elle permet de cacher des informations, d'assurer la confidentialité des messages et de garantir leur authenticité.

Elle réunit la cryptographie et la cryptanalyse

DEFINITIONS

CRYPTOGRAPHIE :

Ensemble des procédés visant à crypter des informations pour en assurer la confidentialité entre l'émetteur et le destinataire.

DEFINITIONS

CRYPTANALYSE :

La cryptanalyse est la technique qui consiste à déduire d'un texte chiffré, un texte en clair sans posséder la clé de chiffrement (l'art de « *casser* » les messages chiffrés).

DEFINITIONS

CRYPTOLOGIE :

La cryptologie est la science du secret. Elle réunit la cryptographie et la cryptanalyse.

CRYPTOGRAPHIE :

Ensemble des procédés visant à crypter des informations pour en assurer la confidentialité entre l'émetteur et le destinataire.

CRYPTANALYSE :

La cryptanalyse est la technique qui consiste à déduire un texte en clair d'un texte chiffré sans posséder la clé de chiffrement (l'art de « *casser* » les messages chiffrés).



CRYPTOLOGIE

Les grands principes de la cryptologie et du chiffrement

CRYPTOLOGIE

La cryptologie ne se limite plus aujourd'hui à assurer la **confidentialité** des secrets. Elle s'est élargie au fait d'assurer mathématiquement d'autres notions :

- Assurer l'**authenticité** d'un message (*qui a envoyé ce message ?*).
- Assurer l'**intégrité** d'un message(*est-ce qu'il a été modifié ?*).

Pour pouvoir jouer ce rôle, la cryptologie regroupe quatre principales fonctions :

CRYPTOLOGIE

La cryptologie ne se limite plus aujourd'hui à assurer la **confidentialité** des secrets. Elle s'est élargie au fait d'assurer mathématiquement d'autres notions :

- Assurer l'**authenticité** d'un message (*qui a envoyé ce message ?*).
- Assurer l'**intégrité** d'un message(*est-ce qu'il a été modifié ?*).

Pour pouvoir jouer ce rôle, la cryptologie regroupe quatre principales fonctions :

- **Le hachage (sans clé).**

CRYPTOLOGIE

La cryptologie ne se limite plus aujourd'hui à assurer la **confidentialité** des secrets. Elle s'est élargie au fait d'assurer mathématiquement d'autres notions :

- Assurer l'**authenticité** d'un message (*qui a envoyé ce message ?*).
- Assurer l'**intégrité** d'un message(*est-ce qu'il a été modifié ?*).

Pour pouvoir jouer ce rôle, la cryptologie regroupe quatre principales fonctions :

- **Le hachage (sans clé).**
- **Le hachage à clé.**

CRYPTOLOGIE

La cryptologie ne se limite plus aujourd'hui à assurer la **confidentialité** des secrets. Elle s'est élargie au fait d'assurer mathématiquement d'autres notions :

- Assurer l'**authenticité** d'un message (*qui a envoyé ce message ?*).
- Assurer l'**intégrité** d'un message(*est-ce qu'il a été modifié ?*).

Pour pouvoir jouer ce rôle, la cryptologie regroupe quatre principales fonctions :

- **Le hachage (sans clé).**
- **Le hachage à clé.**
- **La signature numérique.**

CRYPTOLOGIE

La cryptologie ne se limite plus aujourd'hui à assurer la **confidentialité** des secrets. Elle s'est élargie au fait d'assurer mathématiquement d'autres notions :

- Assurer l'**authenticité** d'un message (*qui a envoyé ce message ?*).
- Assurer l'**intégrité** d'un message(*est-ce qu'il a été modifié ?*).

Pour pouvoir jouer ce rôle, la cryptologie regroupe quatre principales fonctions :

- **Le hachage (sans clé).**
- **Le hachage à clé.**
- **La signature numérique.**
- **Le chiffrement.**



CRYPTOLOGIE

Pourquoi la cryptologie existe-t-elle ?

POURQUOI LA CRYPTOLOGIE EXISTE-T-ELLE ?

➤ Pour assurer l'intégrité du message : ***Le hachage***

POURQUOI LA CRYPTOLOGIE EXISTE-T-ELLE ?

- Pour assurer l'intégrité du message : ***Le hachage***
- Pour assurer l'authenticité du message : ***La signature***

POURQUOI LA CRYPTOLOGIE EXISTE-T-ELLE ?

- Pour assurer l'intégrité du message : ***Le hachage***
- Pour assurer l'authenticité du message : ***La signature***
- Pour assurer la confidentialité du message : ***Le chiffrement***

LA HACHAGE

(Assurer l'intégrité du message)





LA HACHAGE

(Assurer l'intégrité du message)

Opération qui consiste à appliquer une fonction mathématique permettant de créer l'empreinte numérique d'un message, en transformant un message de taille variable en un code de taille fixe, en vue de son authentification ou de son stockage.

LE HACHAGE : *ASSURER L'INTÉGRITÉ DU MESSAGE*

La cryptologie permet justement de détecter si le message, ou l'information, a été involontairement modifié. Ainsi, une « **fonction de hachage** » permettra d'associer à un message, à un fichier ou à un répertoire, une empreinte unique calculable et vérifiable par tous. Cette empreinte est souvent matérialisée par une longue suite de chiffres et de lettres précédées du nom de l'algorithme utilisé, par exemple « **SHA2** » ou « **SHA256** ».

LE HACHAGE : *ASSURER L'INTÉGRITÉ DU MESSAGE*

Il ne faut pas confondre le chiffrement, qui permet d'assurer la confidentialité, c'est-à-dire que seules les personnes visées peuvent y avoir accès, et le hachage qui permet de garantir que le message est intègre, c'est-à-dire qu'il n'a pas été modifié.

Cas d'utilisation :

- *Pour sauvegarder ses photos sur un espace d'hébergement (de type « cloud » par exemple) et vérifier que le téléchargement s'est bien déroulé ?*
- *Pour synchroniser ses dossiers et détecter ceux qu'il faut sauvegarder à nouveau et ceux qui n'ont pas été modifiés ?*

LE HACHAGE : *ASSURER L'INTÉGRITÉ DU MESSAGE*

Il existe aussi des « **fonctions de hachage à clé** » qui permettent de rendre le calcul de l'empreinte différent en fonction de la clé utilisée. Avec celles-ci, pour calculer une empreinte, on utilise une clé secrète. Pour deux clés différentes l'empreinte obtenue sur un même message sera différente. Donc pour que deux personnes calculent la même empreinte, ils doivent tous les deux utiliser la même clé.

LE HACHAGE : *ASSURER L'INTÉGRITÉ DU MESSAGE*

C'est parmi ces fonctions de hachage à clé que l'on trouve celles utilisées pour stocker les mots de passe de façon sécurisée.

Cas d'utilisation :

- *Quand une plateforme « préféré » reconnaît votre mot de passe quand vous vous connectez ?*
- *Quand vous voulez pouvoir détecter si quelqu'un modifie des documents sans vous le dire ?*

COMMENT FONCTIONNENT LES FONCTIONS DE HACHAGE ET HACHAGE A CLÉ ?

COMMENT FONCTIONNENT LES FONCTIONS DE HACHAGE ET HACHAGE A CLÉ ?

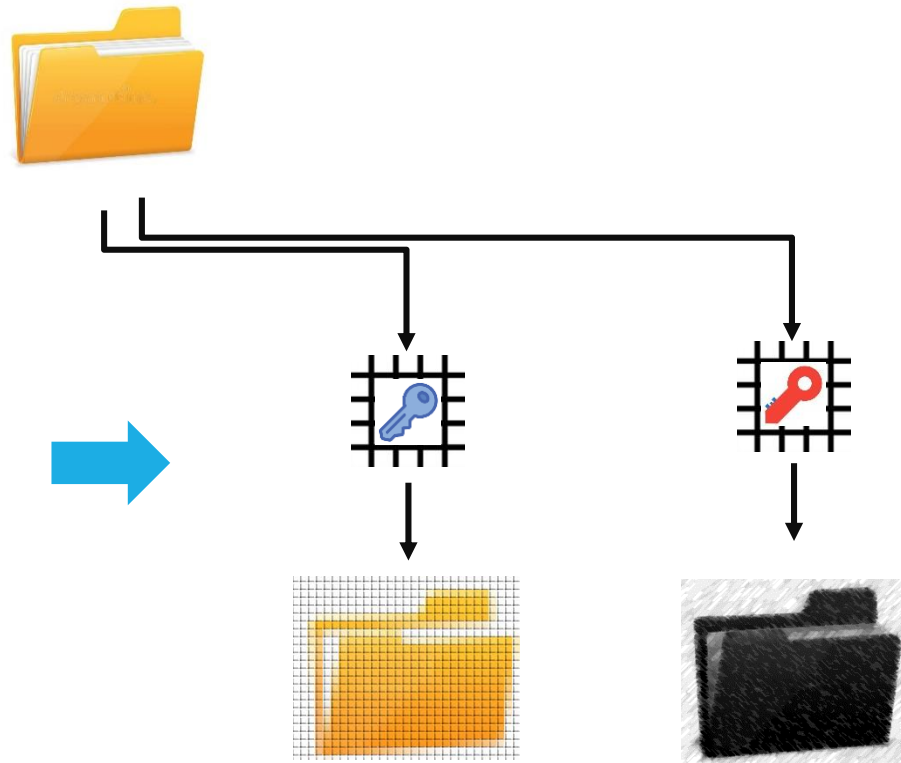


Une fonction de hachage calcule l'empreinte du document (message, fichier, dossier) qui lui est passé, Cette empreinte est une sorte d'identifiant unique du document généré à un moment précis.

← HACHAGE

COMMENT FONCTIONNENT LES FONCTIONS DE HACHAGE ET HACHAGE A CLÉ ?

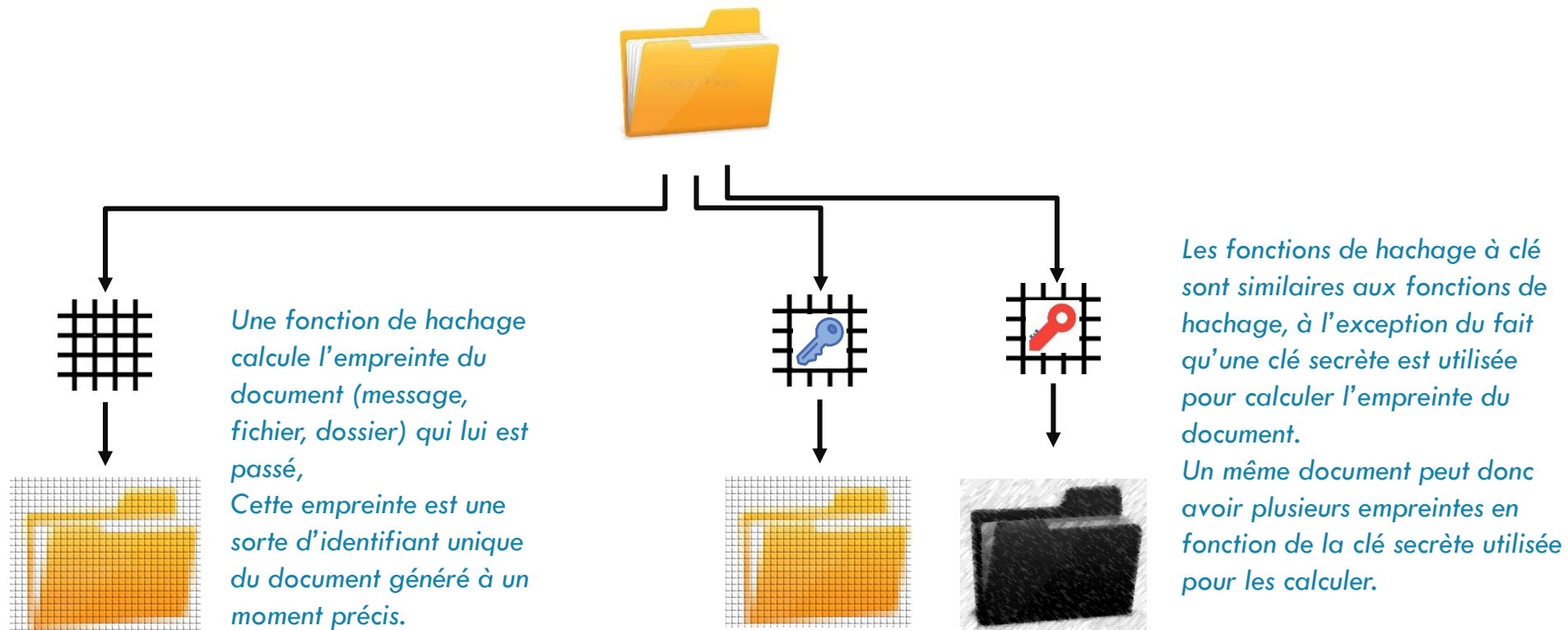
HACHAGE
A CLÉ



Les fonctions de hachage à clé sont similaires aux fonctions de hachage, à l'exception du fait qu'une clé secrète est utilisée pour calculer l'empreinte du document.

Un même document peut donc avoir plusieurs empreintes en fonction de la clé secrète utilisée pour les calculer.

COMMENT FONCTIONNENT LES FONCTIONS DE HACHAGE ET HACHAGE A CLÉ ?



CAS PRATIQUE



COMMENT FONCTIONNENT LES FONCTIONS DE HACHAGE ET HACHAGE A CLÉ ?

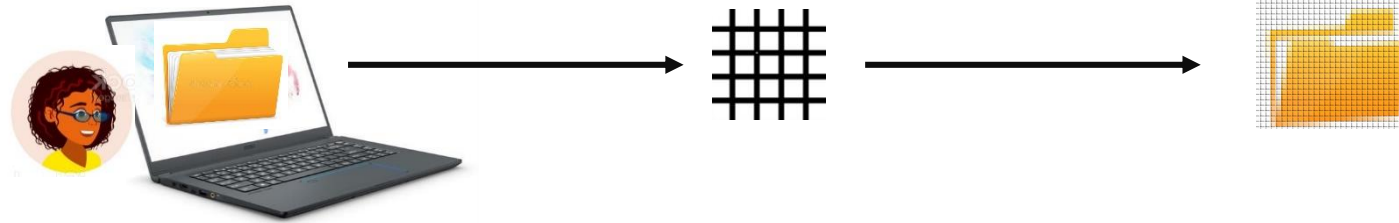
Alice veut charger un de ses fichiers sur le Cloud et veut être sûre que son fichier n'a pas été altéré lors du transfert.



COMMENT FONCTIONNENT LES FONCTIONS DE HACHAGE ET HACHAGE A CLÉ ?

Alice veut charger un de ses fichiers sur le Cloud et veut être sûre que son fichier n'a pas été altéré lors du transfert.

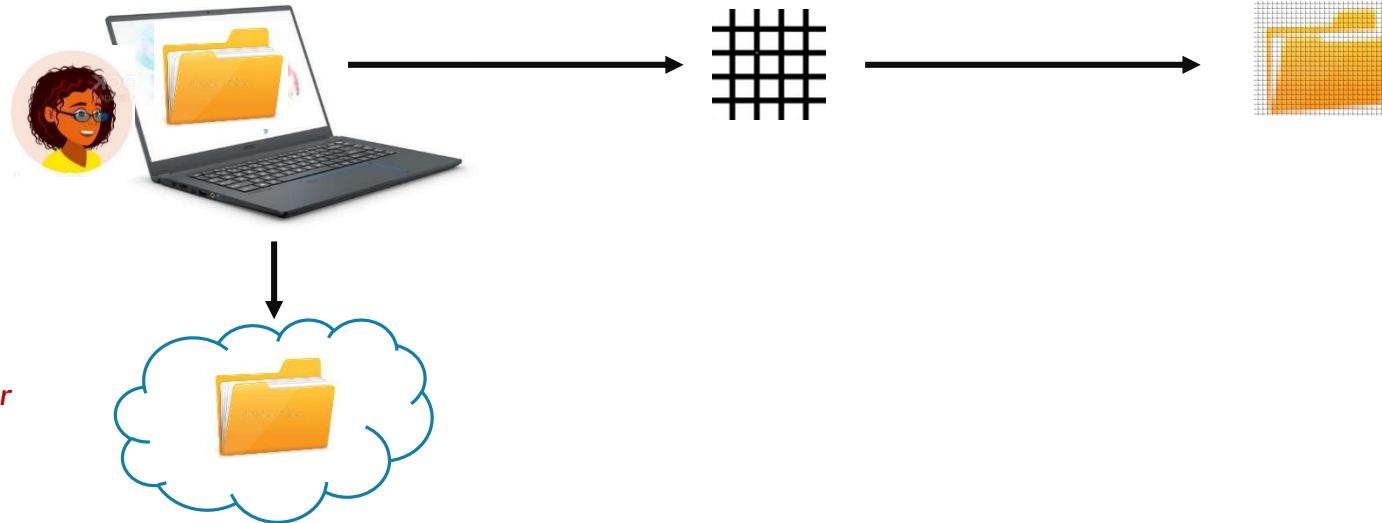
1 - Elle va d'abord calculer l'empreinte du fichier sur son ordinateur.



COMMENT FONCTIONNENT LES FONCTIONS DE HACHAGE ET HACHAGE A CLÉ ?

Alice veut charger un de ses fichiers sur le Cloud et veut être sûre que son fichier n'a pas été altéré lors du transfert.

1 - Elle va d'abord calculer l'empreinte du fichier sur son ordinateur.

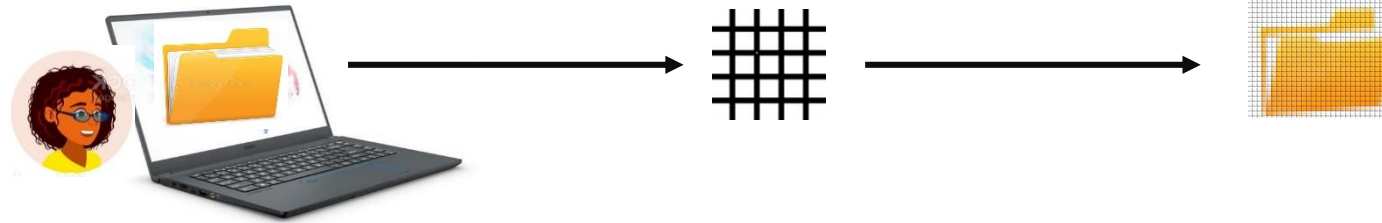


2 - Ensuite elle charge le fichier sur le Cloud.

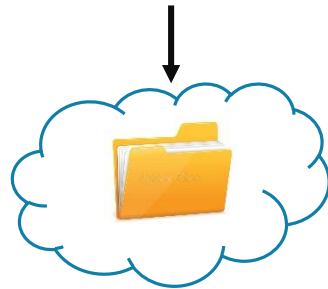
COMMENT FONCTIONNENT LES FONCTIONS DE HACHAGE ET HACHAGE A CLÉ ?

Alice veut charger un de ses fichiers sur le Cloud et veut être sûre que son fichier n'a pas été altéré lors du transfert.

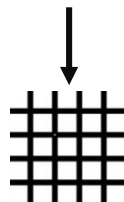
1 - Elle va d'abord calculer l'empreinte du fichier sur son ordinateur.



2 - Ensuite elle charge le fichier sur le Cloud.



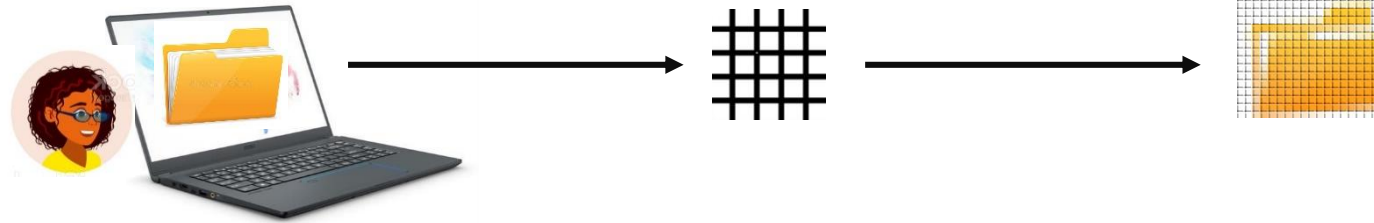
3 - Le fichier chargé, elle calcule alors l'empreinte du fichier chargé.



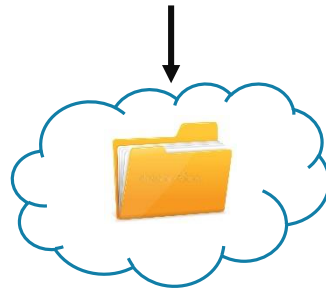
COMMENT FONCTIONNENT LES FONCTIONS DE HACHAGE ET HACHAGE A CLÉ ?

Alice veut charger un de ses fichiers sur le Cloud et veut être sûre que son fichier n'a pas été altéré lors du transfert.

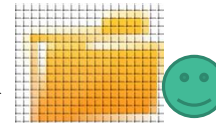
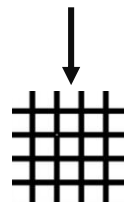
1 - Elle va d'abord calculer l'empreinte du fichier sur son ordinateur.



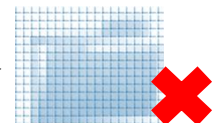
2 - Ensuite elle charge le fichier sur le Cloud.



3 - Le fichier chargé, elle calcule alors l'empreinte du fichier chargé.



4 - Alice compare les deux fichiers pour savoir si une modification involontaire a eu lieu ou non.



LA SIGNATURE

(Assurer l'authenticité du message)



LA SIGNATURE : *ASSURER L'AUTHENTICITÉ DU MESSAGE*

Au même titre que pour un document administratif ou un contrat sur support papier, le mécanisme de la « **signature** » - numérique - permet de vérifier qu'un message a bien été envoyé par le détenteur d'une « clé publique ». Ce procédé cryptographique permet à toute personne de s'assurer de l'identité de l'auteur d'un document et permet en plus d'assurer que celui-ci n'a pas été modifié.

Cas d'utilisation :

- Lorsque l'on veut garantir être l'émetteur d'un courriel ?
- Lorsque l'on veut s'assurer qu'une information provient d'une source sûre ?

LA SIGNATURE : *ASSURER L'AUTHENTICITÉ DU MESSAGE*

Pour pouvoir signer, Alice doit se munir d'une paire de clés :

l'une, dite « *publique* », qui peut être accessible à tous et en particulier à Bob qui est le destinataire des messages qu'envoie Alice ;

l'autre, dite « *privée* », qui ne doit être connue que d'Alice.

En pratique, Alice génère sa signature avec sa clé privée qui n'est connue que d'elle.

N'importe quelle personne ayant accès à la clé publique d'Alice, dont Bob, peut vérifier la signature sans échanger de secret.

COMMENT FONCTIONNE LES SIGNATURES NUMÉRIQUES ?

Ce procédé cryptographique permet à toute personne de s'assurer de l'identité de l'auteur d'un document et permet en plus de s'assurer que celui-ci n'a pas été modifié.

Le procédé repose sur un couple de clés : l'une est privée et connue uniquement de son détenteur, l'autre est publique et accessible à tous.

La signature est générée en utilisant la clé privée. La clé publique est utilisée pour vérifier cette signature. Cette vérification peut donc être effectuée par n'importe quelle personne ayant accès à la clé publique.

COMMENT FONCTIONNE LES SIGNATURES NUMÉRIQUES ?

Ce procédé cryptographique permet à toute personne de s'assurer de l'identité de l'auteur d'un document et permet en plus de s'assurer que celui-ci n'a pas été modifié.

Le procédé repose sur un couple de clés : l'une est privée et connue uniquement de son détenteur, l'autre est publique et accessible à tous.

La signature est générée en utilisant la clé privée. La clé publique est utilisée pour vérifier cette signature. Cette vérification peut donc être effectuée par n'importe quelle personne ayant accès à la clé publique.



CAS PRATIQUE



COMMENT FONCTIONNE LES SIGNATURES NUMÉRIQUES ?

Alice vient de publier un nouveau logiciel et souhaite assurer à ses futurs utilisateurs l'authenticité des copies qu'ils obtiennent.



COMMENT FONCTIONNE LES SIGNATURES NUMÉRIQUES ?

Alice vient de publier un nouveau logiciel et souhaite assurer à ses futurs utilisateurs l'authenticité des copies qu'ils obtiennent.

1 - Avant de publier librement son logiciel, Alice prend soin de le signer.



COMMENT FONCTIONNE LES SIGNATURES NUMÉRIQUES ?

Alice vient de publier un nouveau logiciel et souhaite assurer à ses futurs utilisateurs l'authenticité des copies qu'ils obtiennent.

1 - Avant de publier librement son logiciel, Alice prend soin de le signer.



2 - Bob vient de télécharger une copie du logiciel mais il veut s'assurer que cette copie provient bien d'Alice.



COMMENT FONCTIONNE LES SIGNATURES NUMÉRIQUES ?

Alice vient de publier un nouveau logiciel et souhaite assurer à ses futurs utilisateurs l'authenticité des copies qu'ils obtiennent.

1 - Avant de publier librement son logiciel, Alice prend soin de le signer.



2 - Bob vient de télécharger une copie du logiciel mais il veut s'assurer que cette copie provient bien d'Alice.



3 - Bob utilise la clé publique d'Alice pour vérifier la signature de la copie.

COMMENT FONCTIONNE LES SIGNATURES NUMÉRIQUES ?

Alice vient de publier un nouveau logiciel et souhaite assurer à ses futurs utilisateurs l'authenticité des copies qu'ils obtiennent.

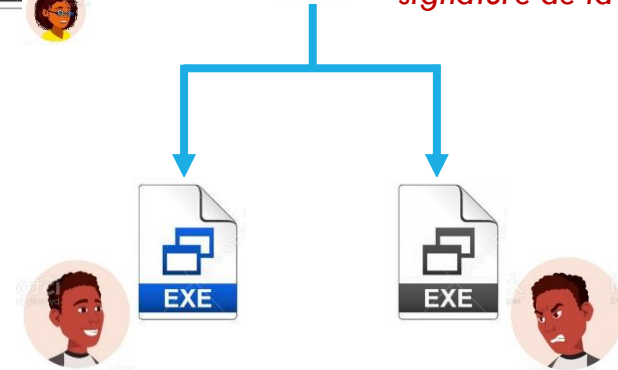
1- Avant de publier librement son logiciel, Alice prend soin de le signer.



2- Bob vient de télécharger une copie du logiciel mais il veut s'assurer que cette copie provient bien d'Alice.



3- Bob utilise la clé publique d'Alice pour vérifier la signature de la copie.



4- Si la clé reconnaît la signature, alors c'est une bonne copie !
Dans le cas contraire, Bob préfère ne pas prendre de risques. Il supprimera la copie.

LE CHIFFREMENT

(Assurer la confidentialité du message)



LE CHIFFREMENT : *POUR ASSURER LA CONFIDENTIALITÉ DU MESSAGE*

Le chiffrement d'un message permet de garantir que seuls l'émetteur et le(s) destinataire(s) légitime(s) d'un message en connaissent le contenu. C'est une sorte d'enveloppe scellée numérique. Une fois chiffré, si l'on ne possède pas la clé spécifique, un message est inaccessible et illisible, que ce soit par les humains ou les machines.

Cas d'utilisation :

- *Vous voulez vous assurer que seul le destinataire ait accès au message ?*
- *Vous souhaitez envoyer ces informations sous enveloppe numérique et non lisible par tous comme sur une carte postale ?*

LE CHIFFREMENT : *POUR ASSURER LA CONFIDENTIALITÉ DU MESSAGE*

Il existe deux grandes familles de chiffrement :

LE CHIFFREMENT : *POUR ASSURER LA CONFIDENTIALITÉ DU MESSAGE*

Il existe deux grandes familles de chiffrement :

➤ Le chiffrement symétrique

LE CHIFFREMENT : *POUR ASSURER LA CONFIDENTIALITÉ DU MESSAGE*

Il existe deux grandes familles de chiffrement :

- Le chiffrement symétrique
- Le chiffrement asymétrique.

LE CHIFFREMENT : *POUR ASSURER LA CONFIDENTIALITÉ DU MESSAGE*

Il existe deux grandes familles de chiffrement :

- Le chiffrement symétrique
- Le chiffrement asymétrique.
- *Le chiffrement hybride*

LE CHIFFREMENT : *POUR ASSURER LA CONFIDENTIALITÉ DU MESSAGE*

➤ Le chiffrement symétrique

Le **chiffrement symétrique** permet de chiffrer et de déchiffrer un contenu avec la même clé, appelée alors la « *clé secrète* ». Le chiffrement symétrique est particulièrement rapide mais nécessite que l'émetteur et le destinataire se mettent d'accord sur une clé secrète commune ou se la transmettent par un autre canal. Celui-ci doit être choisi avec précautions, sans quoi la clé pourrait être récupérée par les mauvaises personnes, ce qui n'assurerait plus la confidentialité du message.

CAS PRATIQUE



COMMENT FONCTIONNE LE CHIFFREMENT SYMÉTRIQUE ?

Alice vient d'enregistrer la liste des cadeaux de Noel de sa famille sur l'ordinateur familial. Elle souhaite être la seule à pouvoir y accéder.



COMMENT FONCTIONNE LE CHIFFREMENT SYMÉTRIQUE ?

Alice vient d'enregistrer la liste des cadeaux de Noel de sa famille sur l'ordinateur familial. Elle souhaite être la seule à pouvoir y accéder.

1 - Pour ce faire, Alice chiffre la liste en utilisant sa clé secrète.



COMMENT FONCTIONNE LE CHIFFREMENT SYMÉTRIQUE ?

Alice vient d'enregistrer la liste des cadeaux de Noel de sa famille sur l'ordinateur familial. Elle souhaite être la seule à pouvoir y accéder.

1 - Pour ce faire, Alice chiffre la liste en utilisant sa clé secrète.



2 - Plus tard dans la journée, Bob trouve la liste et cherche à l'ouvrir.



COMMENT FONCTIONNE LE CHIFFREMENT SYMÉTRIQUE ?

Alice vient d'enregistrer la liste des cadeaux de Noel de sa famille sur l'ordinateur familial. Elle souhaite être la seule à pouvoir y accéder.

1 - Pour ce faire, Alice chiffre la liste en utilisant sa clé secrète.



2 - Plus tard dans la journée, Bob trouve la liste et cherche à l'ouvrir.



3 - malheureusement pour lui, Bob est incapable de lire la liste car il ne possède pas la clé secrète.



COMMENT FONCTIONNE LE CHIFFREMENT SYMÉTRIQUE ?

Alice vient d'enregistrer la liste des cadeaux de Noel de sa famille sur l'ordinateur familial. Elle souhaite être la seule à pouvoir y accéder.

1 - Pour ce faire, Alice chiffre la liste en utilisant sa clé secrète.



2 - Plus tard dans la journée, Bob trouve la liste et cherche à l'ouvrir.



3 - malheureusement pour lui, Bob est incapable de lire la liste car il ne possède pas la clé secrète.



4 - La liste est donc bien protégée. Seule Alice peut réussir à la déchiffrer et la lire !



LE CHIFFREMENT : *POUR ASSURER LA CONFIDENTIALITÉ DU MESSAGE*

➤ Le chiffrement asymétrique

Le **chiffrement asymétrique** suppose que le (futur) destinataire est muni d'une paire de clés (*clé privée*, *clé publique*) et qu'il a fait en sorte que les émetteurs potentiels aient accès à sa clé publique. Dans ce cas, l'émetteur utilise la clé publique du destinataire pour chiffrer le message tandis que le destinataire utilise sa clé privée pour le déchiffrer.

Parmi ses avantages, la clé publique peut être connue de tous et publiée. Seulement, il est nécessaire que les émetteurs aient confiance en l'origine de la clé publique, qu'ils soient sûrs qu'il s'agit bien de celle du destinataire.

CAS PRATIQUE



COMMENT FONCTIONNE LE CHIFFREMENT ASYMÉTRIQUE ?

Alice, hackeuse, vient de découvrir des informations d'intérêt public. Elle veut les transmettre à Bob, journaliste, pour qu'il enquête.



COMMENT FONCTIONNE LE CHIFFREMENT ASYMÉTRIQUE ?

Alice, hackeuse, vient de découvrir des informations d'intérêt public. Elle veut les transmettre à Bob, journaliste, pour qu'il enquête.

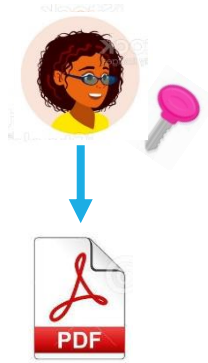
1 - Alice vient de récupérer la clé publique de Bob. Elle l'utilise pour chiffrer son document.



COMMENT FONCTIONNE LE CHIFFREMENT ASYMÉTRIQUE ?

Alice, hackeuse, vient de découvrir des informations d'intérêt public. Elle veut les transmettre à Bob, journaliste, pour qu'il enquête.

1 - Alice vient de récupérer la clé publique de Bob. Elle l'utilise pour chiffrer son document.



2 - Elle l'envoi à Bob.

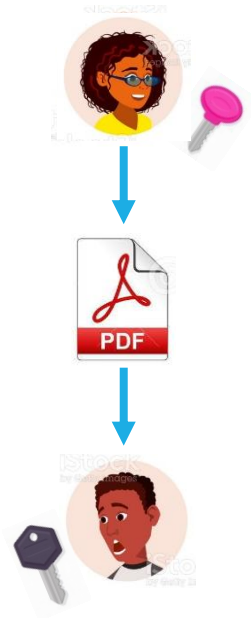
COMMENT FONCTIONNE LE CHIFFREMENT ASYMÉTRIQUE ?

Alice, hackeuse, vient de découvrir des informations d'intérêt public. Elle veut les transmettre à Bob, journaliste, pour qu'il enquête.

1 - Alice vient de récupérer la clé publique de Bob. Elle l'utilise pour chiffrer son document.

2 - Elle l'envoie à Bob.

3 - Bob reçoit le document et le déchiffre à l'aide de sa clé privée.



COMMENT FONCTIONNE LE CHIFFREMENT ASYMÉTRIQUE ?

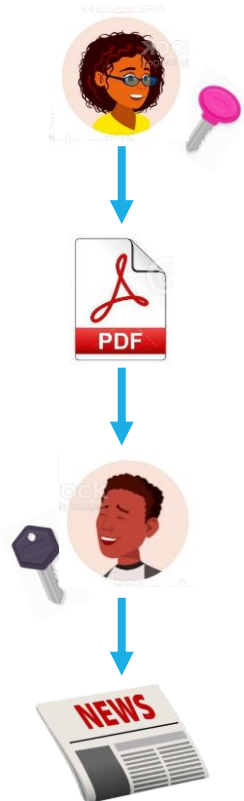
Alice, hackeuse, vient de découvrir des informations d'intérêt public. Elle veut les transmettre à Bob, journaliste, pour qu'il enquête.

1 - Alice vient de récupérer la clé publique de Bob. Elle l'utilise pour chiffrer son document.

2 - Elle l'envoie à Bob.

3 - Bob reçoit le document et le déchiffre à l'aide de sa clé privée.

3 - Une fois le document déchiffré, il rédige un article puis le publie dans son journal.



LE CHIFFREMENT : *POUR ASSURER LA CONFIDENTIALITÉ DU MESSAGE*

Il existe également une autre technique combinant chiffrements « symétrique » et « asymétrique », mieux connue sous le nom de « **chiffrement hybride** ».

LE CHIFFREMENT : *POUR ASSURER LA CONFIDENTIALITÉ DU MESSAGE*

➤ Le chiffrement hybride

Dans ce type de chiffrement, une clé secrète est déterminée par une des deux parties souhaitant communiquer et celle-ci est envoyée chiffrée par un chiffrement asymétrique. Une fois connue des deux parties, celles-ci communiquent en chiffrant symétriquement leurs échanges. Cette technique est notamment appliquée sur les **sites dont l'adresse débute par « [https](#) »**.