Veille technologique : La Cryptographie

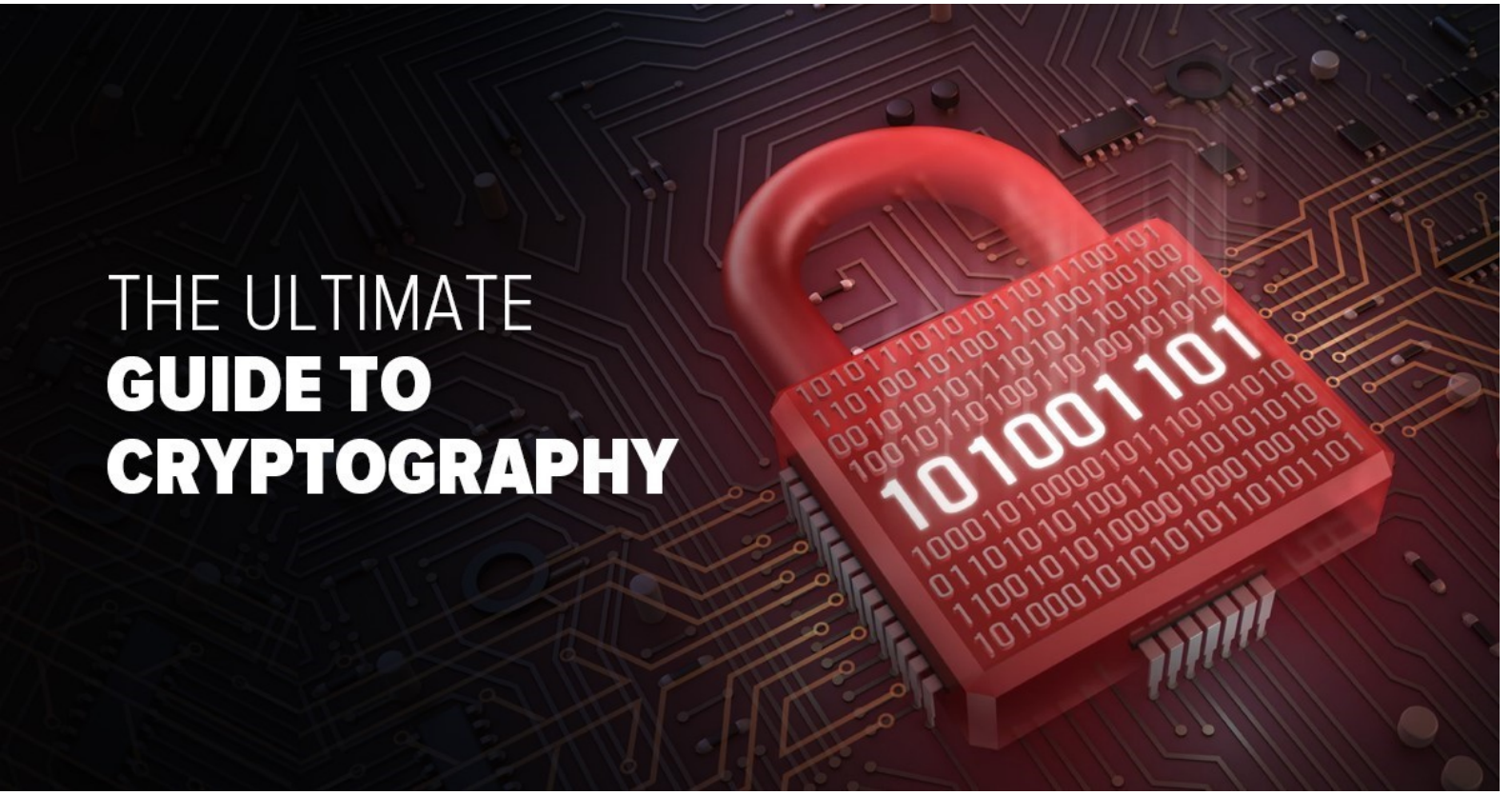


Table des matières

J’ai choisi de faire ma veille technologique sur la cryptographie parce qu’étant toujours attiré par les mathématiques, je me suis vite intéressé au fonctionnement de déchiffrement de messages ainsi qu’au fonctionnement des algorithmes. Après avoir découvert l’informatique lors de ma première année de licence mathématiques-informatique, j’ai voulu orienter ma formation dans l’informatique et le domaine reliant le plus les mathématiques et l’informatique est la **cybersécurité.**

I Introduction

a) Définitions

Le mot cryptographie vient des mots en grec ancien **kruptos** (κρυπτός) « caché » et **graphein** (γράφειν) « écrire ». Beaucoup des termes de la cryptographie utilisent la racine « crypt- », ou des dérivés du terme « chiffre ».

La cryptographie est le fait de transformer un message « normal » en un message **indéchiffrable** pour quiconque ne serait pas le destinataire du message. Ce message est chiffré à l'aide d'un **algorithme**.

Ce chiffrement permet l'échange de données confidentielles et de manière sécurisée, cependant le destinataire doit posséder la **clé** de déchiffrement du message.

La cryptographie permet donc le traitement, le stockage ou la transmission sécurisée de données mais sert aussi pour l'applications de l'authentification et de la signature numérique des messages.

Elle poursuit 4 grands objectifs :

- **La confidentialité**, l'information ne peut être lue par une personne non autorisée
- **L'authenticité**, l'information ne peut prévenir que d'un auteur légitime
- **L'intégrité**, l'information n'est pas modifiable par la personne autre que l'auteur
- **La non-répudiation**, l'information ne peut faire l'objet d'un déni de la part de son auteur

Ces 4 points garantissent une sécurité parfaite à l'utilisateur.

Aujourd'hui, la cryptographie est utilisée partout où des données "sensibles" sont à protéger : dans les administrations, dans les sites militaires, dans les hôpitaux, dans les banques, sur les cartes bancaires et pour une grande partie des transactions sur Internet.

Quelques définitions utiles :

- Algorithme : Suite d'opérations simples qui constituent un procédé utile.
- Chiffre : Synonyme de code afin de chiffrer un message.
- Chiffrage : Processus d'opérations utilisant un algorithme et/ou une clé précise.

- Clé : Paramètre souvent complémentaire à l'algorithme. Elle peut servir à chiffrer, déchiffrer, ou les deux à la fois : la clé est alors appelée symétrique.
- Chiffrement : Fait de rendre non compréhensible un message aux individus non-destinataires de ce message.
- Cryptanalyse : C'est l'étude des systèmes cryptographiques, en particulier de leurs faiblesses, dans le but de déchiffrer les messages dont on n'est pas destinataire.
- Privée (clé) : Clé utilisée par le receveur pour déchiffrer les messages dans un cryptosystème à clé publique. La clé privée doit être tenue secrète.
- Publique (clé) : Clé utilisée par l'envoyeur pour chiffrer les messages dans un cryptosystème à clé publique. La clé publique est disponible pour tout le monde.
- La mécanique quantique : est la théorie mathématique et physique décrivant la structure et l'évolution dans le temps et l'espace des phénomènes physiques à l'échelle de l'atome et en dessous.

b) Histoire

La cryptographie est utilisée depuis aussi longtemps que les hommes savent écrire, l'enjeu de transmettre des informations confidentielles de manières sécurisées est recherché bien avant l'invention d'internet.

Au III^{e} millénaire avant J-C, des hiéroglyphes égyptiens présents sur une tombe auraient reçu des modifications dans le but d'obscurcir le sens des inscriptions.

Le premier moyen de chiffrement connu est le **chiffre de César** inventé au 1er siècle avant J-C**.** Cet algorithme dit de substitution aurait été utilisé par Jules César pour ses correspondances secrètes. Son mode de fonctionnement est ainsi simple, il suffit de remplacer chaque lettre du texte à chiffrer par la lettre qui se situe n places plus loin dans l'alphabet. Par exemple en prenant n=2, on aurait alors A=C, B=D et ainsi de suite…

Plus tard, en 1586 un autre chiffrement célèbre est le **chiffre de Vigénère** (du nom du diplomate français Blaise de Vigenère). Il ressemble au chiffre de César puisqu'il est lui aussi de substitution mais il diffère du fait qu'on utilise une clé plus complexe que le simple remplacement systématique par un décalage de lettres. On utilise un mot clé à

la place. A chaque lettre du texte clair on fait correspondre une lettre de la clé (la clé étant répétée autant de fois que nécessaire). La lettre du texte chiffré sera prise dans la colonne correspondante à la lettre du texte clair, et dans la ligne correspondante à la lettre de la clé.

En posant *C* le texte codé, *T* le texte et *K* la clé, on peut traduire ceci par la formule :

```
C = T + K [mod 26]
```

Pour déchiffrer le message, il suffit de faire l'opération inverse: On prend la ligne correspondant à la lettre de la clé, et on la suit jusqu'à rencontrer le caractère codé ; la lettre décodée est alors la première de cette colonne. Ce qui se traduit par la formule :

```
T = C - K [mod 26]
```

Le chiffrement de Vigenère ne sera cassé qu'en 1854.

Le **chiffrement XOR** appelé également appeler **chiffre de Vernam** ou **masque jetable**, est un algorithme de cryptographie inventé par Gilbert Vernam en 1917 et perfectionné par Joseph Mauborgne, qui rajouta la notion de **clé aléatoire**. Cependant, le banquier américain Frank Miller en avait posé les bases dès 1882. Bien que simple, facile et rapide, tant pour le codage que pour le décodage, ce chiffrement est théoriquement impossible à **casser**, mais le fait que le masque soit à usage unique impose de le transmettre au préalable par un "autre moyen", ce qui soulève des difficultés de mise en œuvre pour la sécurisation des échanges sur Internet.

Le XOR est un opérateur logique qui correspond à un "**OU exclusif**" : c'est le (A OU B) qu'on utilise en logique mais qui exclue le cas où A et B sont simultanément vrais. Voici sa table de vérité :

Table de vérité du XOR		
A	**B**	**(A XOR B)**
FAUX	FAUX	FAUX
FAUX	VRAI	VRAI
VRAI	FAUX	VRAI
VRAI	VRAI	FAUX

En informatique, chaque caractère du message à coder est représenté par un entier, le code ASCII. Ce nombre est lui-même représenté en mémoire comme un nombre binaire à 8 chiffres (les bits). On choisit une clé que l'on place en dessous du message à coder, en la répétant autant de fois que nécessaire, comme dans le chiffrement de Vigenère. Le message et la clé étant converti en binaire, on effectue un XOR, bit par bit, le 1 représentant VRAI et le 0 FAUX. Le résultat en binaire peut être reconverti en caractères ASCII et donne alors le message codé. L'algorithme est complètement symétrique : la même opération est réappliquée au message final pour retrouver le message initial.

Le chiffrement D.E.S.

En détail plus loin

Le système de cryptographie R.S.A

En détail plus loin

Dans l'histoire, beaucoup de codes étaient considérés comme inviolables mais ont été cassés (Vigenère, Enigma, ...). Les systèmes actuels à clés publiques sont-ils alors menacés ? Quoi qu'il en soit, on se tourne maintenant vers une nouvelle sorte de cryptographie, ne reposant pas sur l'aspect déterministe des mathématiques, mais sur l'aspect probabiliste de la physique. Ces travaux se basent sur les recherches de Stephen Wiesner dans les années 60, qui inventa le principe de cryptographie quantique.
Le message est transmis par des photons polarisés.

Les activités de cryptographie ont en grande partie servi le secteur militaire et sont longtemps restées classées secret Défense.

L'ouverture de la cryptographie au monde civil fut décisive pour son évolution.
Le 15 mai 1973 le **NBS** (*National Bureau of Standards*) a lancé un appel pour la création d'un algorithme de chiffrement répondant aux critères suivants :

- Posséder un haut niveau de sécurité lié à une clé de petite taille servant au chiffrement et au déchiffrement
- Être compréhensible
- Ne pas dépendre de la confidentialité de l'algorithme
- Être adaptable et économique
- Être efficace et exportable

Fin 1974, IBM propose « Lucifer », qui, grâce à la NSA (National Security Agency), est modifié le 23 novembre 1976 pour donner le DES (Data Encryption Standard). Le DES a finalement été approuvé en 1978 par le NBS. Le DES fut normalisé par

l'ANSI (American National Standard Institute) sous le nom de ANSI X3.92, plus connu sous la dénomination DEA (Data Encryption Algorithm).

II Chiffrement symétrique

a) Introduction

C'est ainsi que fut créé l'un des premiers algorithmes de chiffrement spécifiquement conçu pour être utilisé dans le secteur privé.

La cryptographie symétrique, également dite à clé secrète (par opposition à la cryptographie asymétrique), est la plus ancienne forme de chiffrement. Elle permet à la fois de chiffrer et de déchiffrer des messages à l'aide d'un même mot clé. On a des traces de son utilisation par les Égyptiens vers 2000 av. J.-C.

Il s'agit d'un système de chiffrement symétrique par blocs de 64 bits, dont 8 bits (un octet) servent de test de parité (pour vérifier l'intégrité de la clé). Chaque bit de parité de la clé (1 tous les 8 bits) sert à tester un des octets de la clé par parité impaire, c'est-à-dire que chacun des bits de parité est ajusté de façon à avoir un nombre impair de '1' dans l'octet à qui il appartient. La clé possède donc une longueur « utile » de 56 bits, ce qui signifie que seuls 56 bits servent réellement dans l'algorithme.

Le standard de chiffrement symétrique actuel AES est le résultat d'un concours académique lancé en 1997 par le National Institute of Standards and Technology (NIST) américain. 16 équipes de cryptologues venues du monde entier ont participé à cette compétition publique. En 2000, l'algorithme proposé par une équipe belge remporte la compétition et vient donc remplacer le Data Encryption Standard (DES), le standard précédent.

Pour la première fois, la sélection est réalisée publiquement par l'ensemble des experts du domaine selon un processus plus transparent qu'auparavant dont la finalité est de sélectionner l'algorithme présentant les meilleures garanties.

b) Utilisation en informatique

Dans le secteur bancaire. Compte tenu des meilleures performances et de la vitesse plus rapide du chiffrement symétrique, la cryptographie symétrique est

généralement employée pour chiffrer en masse de grandes quantités de données. Les applications du chiffrement symétrique dans le secteur de la banque comprennent :

Les applications de paiement, notamment les transactions par carte lors desquelles les données personnelles doivent être protégées de manière à éviter les vols d'identité et les opérations frauduleuses sans engager de ressources extrêmement couteuses. Cette méthode permet de réduire les risques liés à la gestion des transactions de paiement quotidiennes.

En outre, la cryptographie symétrique assure uniquement la confidentialité des données transmises ou stockées. Elle ne peut pas être employée pour confirmer leur intégrité ni leur authenticité.

III Chiffrement asymétrique

a) Introduction

En cryptographie asymétrique, au lieu de faire reposer la sécurité sur un secret partagé, c'est à dire n'avoir qu'une seule clé comme c'est le cas en cryptographie symétrique, on dispose d'un couple de clés que l'on appelle bi-clé. L'une d'elle est privée et l'autre publique. Utilisant des fonctionnements mathématiques, ce qui est chiffré avec la clé publique ne peut être déchiffré qu'avec la clé privée. À la différence de la clé publique, cette dernière doit par définition rester secrète et ne pas quitter son propriétaire.

La cryptographie à clé publique sert de moyen d'assurer la confidentialité, l'authenticité et la non-répudiation des communications et du stockage de données électroniques.

La paire de clés se base sur de très longs chiffres premiers. La clé publique et la clé privée sont calculées ensemble simultanément au cours d'un même calcul mathématique faisant appel à des fonctions « à trappe ». La principale caractéristique de ce type de fonctions réside dans le fait qu'elles sont très simples à calculer dans un sens, mais difficiles à calculer dans l'autre (en trouvant leur inverse) en l'absence d'informations spécifiques.

Le principal inconvénient du chiffrement asymétrique est sa lenteur par rapport au chiffrement symétrique. En effet, le chiffrement asymétrique exige une puissance de

calcul bien supérieure en raison de sa complexité mathématique. Il ne convient pas aux longues sessions du fait de la puissance de traitement qu'il nécessite pour perdurer.

En 1978, l'algorithme à clé publique de Rivest, Shamir et Adelman (R.S.A.) nommé par les initiales de ses trois inventeurs, apparaît. Il servait encore au début du XXIème siècle à protéger les codes nucléaires des armées américaines et soviétiques.

Basé sur la difficulté de factoriser de grands entiers, l'algorithme du système R.S.A. peut se résumer à 5 étapes :

1) Choisir deux grands nombres premiers p et q de plus de 80 chiffres (en dessous, le code est vulnérable)
2) Calculer n=p.q et f=(p-1).(q-1)
3) Choisir un nombre e premier avec f et n (i.e. tel que pgcd(e,f.n)=1
4) Trouver d tel que $e.d \equiv 1 \ [f]$
5) Le message à chiffrer est converti en blocs de chiffres B_i, tous inférieurs à n. Pour chiffrer le bloc B_i, on calcule B_i^e modulo n.

Il faut savoir qu'un mauvais choix des paramètres p, q, d et e peut rendre le système relativement vulnérable. Pour cela, les concepteurs du système ont proposé un certain nombre de règles :

- Il faut choisir n = p.q de taille supérieure ou égale à 512 bits (155 chiffres décimaux environ).

- Il faut prendre p et q de taille sensiblement égale, mais pas trop proches en valeur absolue.

- Il faut choisir, si possible, des nombres premiers p et q, tels que p-1, p+1, q-1 et q+1 possèdent de grands facteurs premiers.

La sécurité du système RSA se base sur le fait qu'il y a une impossibilité pratique de factoriser un grand nombre de quelques centaines de chiffres en un temps raisonnable : Selon R.S.A., factoriser un nombre à 200 chiffres demande 4 milliards d'années de calcul machine. Factoriser un nombre de 500 chiffres demande 1025 ans. La robustesse du R.S.A. apparaît donc liée à la difficulté de la factorisation avec les méthodes actuelles.

b) Utilisation informatique

Pour assurer l'authenticité du message : la signature

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.

La signature numérique, pour quoi faire ?
Pour garantir être l'émetteur d'un courriel.
S'assurer qu'une information provient d'une source sûre.

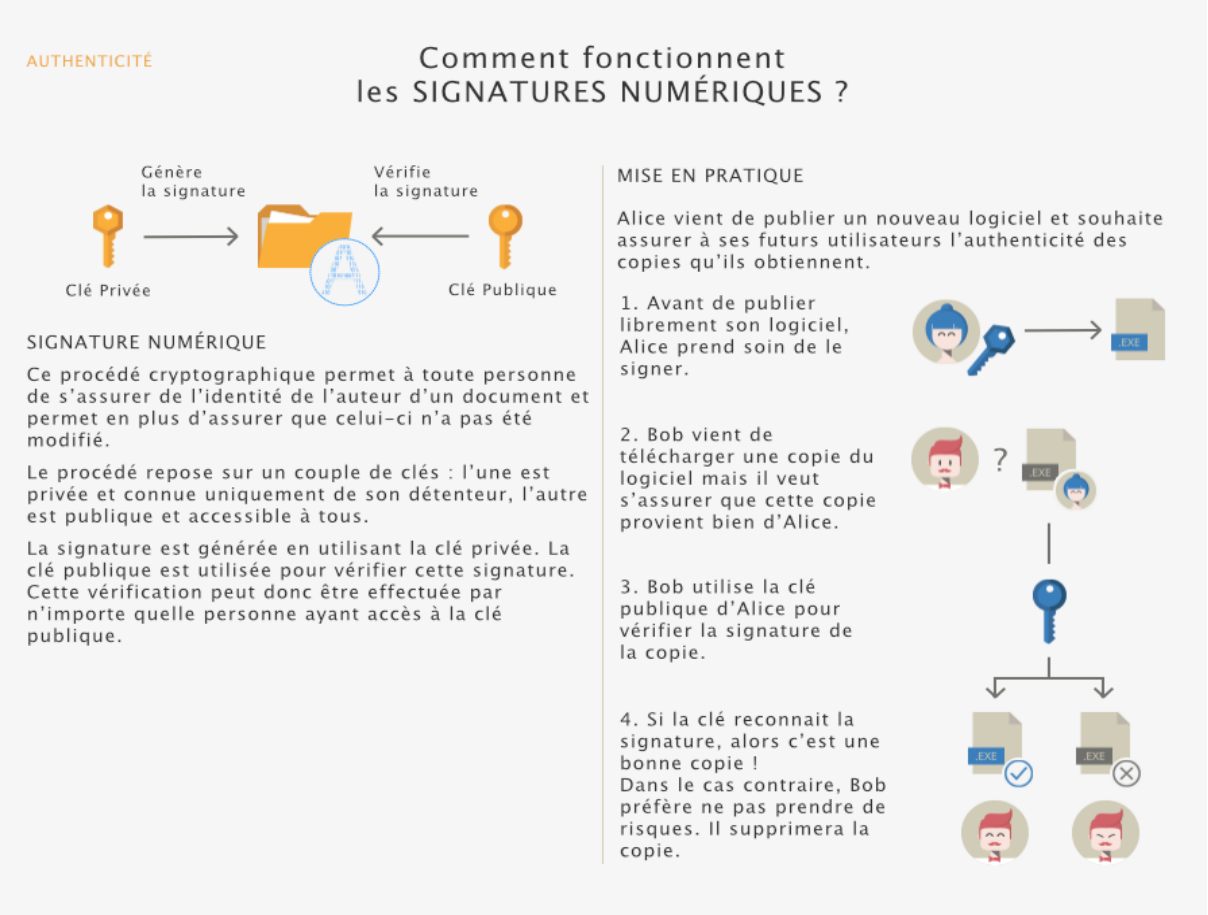
Pour expliquer la cryptologie, nous utiliserons dans nos exemples les personnages traditionnels en cryptographie : Alice et Bob.

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.

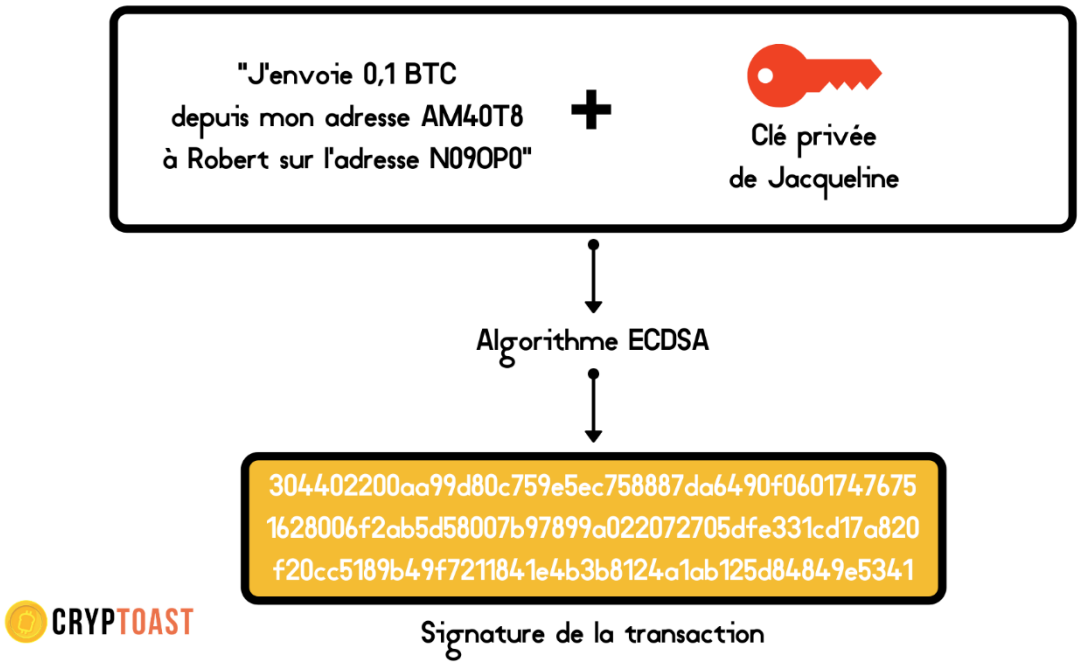


Dans le bitcoin

Comme quand elle fait un chèque en euros, Jacqueline va devoir signer sa transaction pour authentifier auprès du réseau le fait qu'elle en est à l'origine.

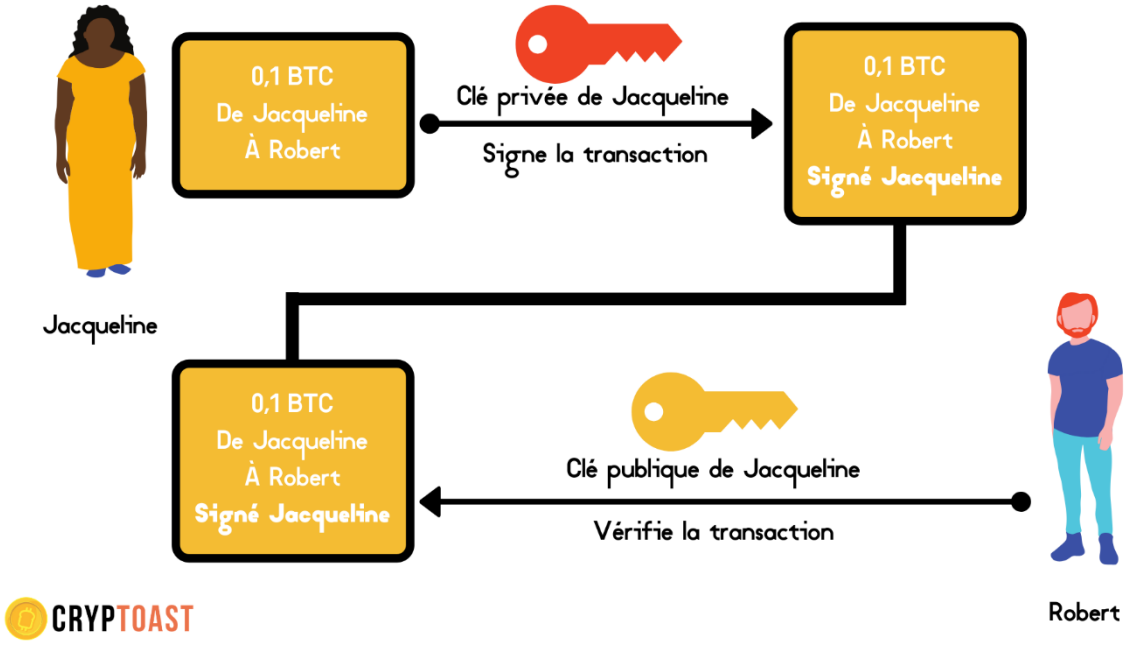
Pour cela, Bitcoin utilise un algorithme de signature numérique (appelé ECDSA) qui signe les transactions à l'aide de la clé privée de l'émetteur.

La signature est une chaîne de caractères incompréhensible pour le commun des mortels. Elle est générée grâce à l'algorithme en utilisant la clé privée de Jacqueline et son message. Par exemple :



Grâce à l'algorithme, n'importe qui peut vérifier que cette signature a bien été générée par Jacqueline pour effectuer cette transaction. Pour cela, il faut utiliser le même algorithme avec la signature, la clé publique de Jacqueline et le message de la transaction qu'elle a émis.

Ainsi, tout le monde (dont Robert) peut s'assurer que c'est bien elle qui est à l'origine de la transaction de 0,1 BTC de son portefeuille vers celui de Robert.



L'utilisation de la cryptographie asymétrique apporte deux éléments à Bitcoin. Les transactions sont impossibles à falsifier car elles sont signées par la clé privée de

l'émetteur. De plus, l'auteur de celle-ci ne peut pas nier avoir fait cette dépense, puisqu'il est le seul à avoir pu la crypter ainsi.

C'est pour cette raison qu'il est essentiel de tenir secrète votre clé privée. Vous ne devez en aucun cas la communiquer. Sinon, vos fonds ne vous appartiennent plus, car quiconque pourra signer des transactions à votre place.

IV Chiffrement hybride

Pour assurer la confidentialité du message : le chiffrement

Le chiffrement d'un message permet justement 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, faute d'avoir la clé spécifique, un message est inaccessible et illisible, que ce soit par les humains ou les machines.

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.

CONFIDENTIALITÉ

Comment fonctionne le CHIFFREMENT ?

CHIFFREMENT SYMÉTRIQUE

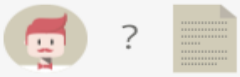
Le chiffrement symétrique permet de chiffrer et déchiffrer un fichier avec la même clé, dite secrète. Pour s'échanger un message il faut donc que les deux parties partagent la même clé.

MISE EN PRATIQUE

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

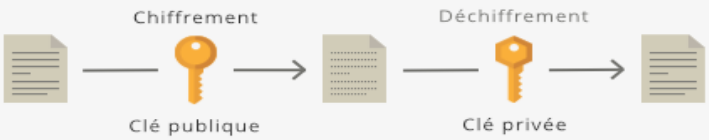
1. Pour ce faire, Alice chiffre la liste en utilisant sa clé secrète.

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 !



CHIFFREMENT ASYMÉTRIQUE

Le chiffrement asymétrique repose sur l'utilisation d'une paire de clés : une publique et une privée.

La clé publique, accessible à tous, est utilisée pour chiffrer les fichiers. Seule la clé privée permet de déchiffrer ces fichiers, celle-ci étant connue que d'un seul individu.

MISE EN PRATIQUE

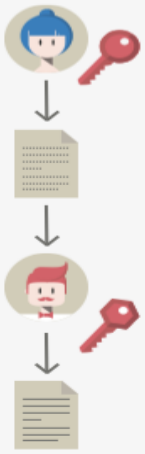
Alice, hackeuse, vient de découvrir des informations d'intérêt public. Elle veut les transmettre à Bob, journaliste, pour qu'il enquête.

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.

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



Parmi ses avantages, la clé publique peut être connue de tous et publiée. Mais attention : 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.

Autre point fort : plus besoin de partager une même clé secrète ! Le chiffrement asymétrique permet de s'en dispenser. Mais il est malheureusement plus lent.

Pour cette dernière raison, il existe une technique combinant chiffrements « symétrique » et « asymétrique », mieux connue sous le nom de « chiffrement hybride ».

Cette fois, 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 lorsque vous visitez un site dont l'adresse débute par « https ».

Le protocole HTTPS est utilisé pour l'identification des machines. Au sein d'un monde étroitement connecté où des millions de données sensibles sont transmises chaque jour via Internet, la nécessité de sécuriser les canaux de communication entre les clients/navigateurs et les serveurs revêt la plus grande importance.

Protocole de la couche d'application TCP/IP, HTTPS est en fait le protocole de sécurité SSL/TLS exécuté au-dessus d'HTTP. Une connexion HTTPS entre un client et un serveur emploie deux types de chiffrement. Le chiffrement asymétrique est d'abord utilisé pour établir la connexion, avant d'être remplacé par le chiffrement symétrique (appelé « session ») pendant la durée de la connexion. Une clé de session est une clé symétrique à usage unique utilisée pour le chiffrement et le déchiffrement. Les clés de session sont créées aléatoirement et uniquement employées durant une session donnée.

Voici comment HTTPS fonctionne en quelques étapes simples :

1. Avant que le serveur et le client n'établissent une conversation sécurisée, un certificat TLS doit être créé et vérifié par l'autorité de certification (CA).
2. Le navigateur envoie un message ClientHello pour indiquer qu'il souhaite initier une conversation avec un serveur sécurisé. Le message ClientHello contient toutes les informations nécessaires au serveur pour se connecter au client via TLS, y compris les différentes suites de chiffrement et la version TLS maximale qu'il prend en charge.
3. Le serveur répond par un message ServerHello, qui indique la version TLS à utiliser ainsi que le certificat TLS et la clé publique asymétrique du serveur.
4. Le navigateur vérifie le certificat du serveur et crée une clé de session aléatoire.
5. La clé de session est chiffrée à l'aide de la clé publique du serveur puis renvoyée au serveur.
6. Le serveur déchiffre la clé de session avec sa propre clé privée.
7. Les deux parties disposent désormais de la clé de session. Le chiffrement à clé publique est terminé et remplacé par le chiffrement symétrique. La session avec

le serveur se poursuit uniquement avec le chiffrement symétrique.

Dans les deux cas précédents (applications de messagerie et HTTPS), le chiffrement asymétrique est uniquement employé brièvement au début pour échanger la clé de session symétrique qui sera utilisée pour le reste de la connexion. Cette méthode a pour fonction de remédier au principal inconvénient du chiffrement asymétrique, à savoir sa lenteur et sa gourmandise en ressources en raison de sa complexité mathématique. D'autre part, le recours au chiffrement asymétrique résout le problème de distribution de clés lié au chiffrement symétrique.

Les applications de messagerie telles que Signal ou Whatsapp emploient un chiffrement de bout en bout afin de protéger la confidentialité des communications des utilisateurs ainsi que pour authentifier ces derniers.

Avec un chiffrement de bout en bout, seules les données sont chiffrées. Les en-têtes, les codes de fin et les informations de routage ne le sont pas. Le fondement du chiffrement de bout en bout est le Signal Protocol conçu par Open Whisper Systems. Ce protocole de chiffrement de bout en bout a été développé pour éviter que les tierces parties et l'opérateur de messagerie ne fournissent un accès aux messages et aux appels en texte en clair. En outre, même si les clés de chiffrement du périphérique d'un utilisateur venaient à être physiquement compromises, il serait impossible de remonter le temps pour déchiffrer les messages précédemment transmis.

Le chiffrement de bout en bout de la messagerie est mis en œuvre à l'aide de la cryptographie symétrique et asymétrique. Le chiffrement asymétrique est employé pour initialiser la conversation chiffrée entre deux utilisateurs, tandis que le chiffrement symétrique est déployé le temps de la communication. Le Livre blanc de synthèse sur le chiffrement Whatsapp en fournit les détails.

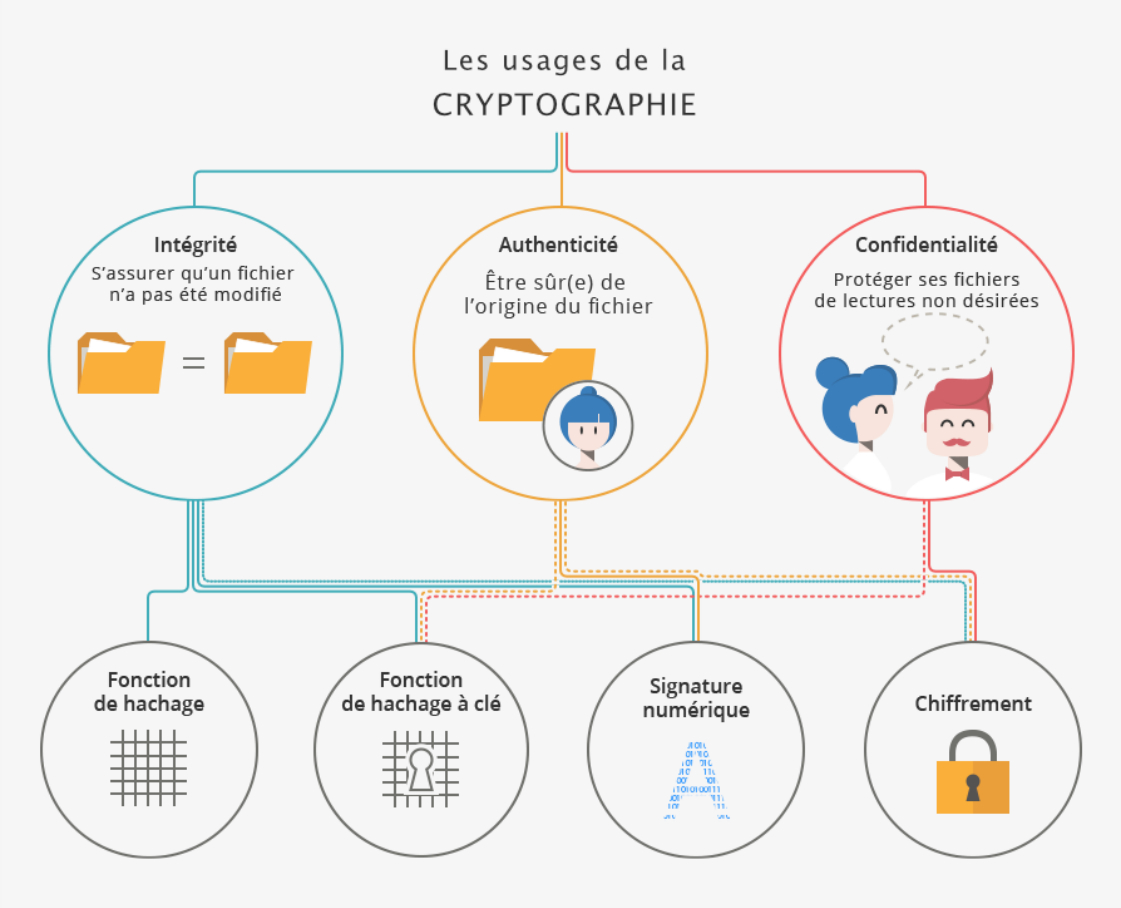
Une fois l'application installée sur le smartphone de l'utilisateur, les clés publiques du client sont enregistrées auprès du serveur de l'application. La clé privée n'est pas stockée sur le serveur et demeure secrète sur le périphérique de l'utilisateur. Le client qui souhaite initier une session récupère les clés publiques du destinataire sur le serveur Whatsapp. À l'aide de ces clés, l'initiateur chiffre le premier message et le transmet au destinataire. Ce message contient les paramètres permettant d'établir une clé de session symétrique. Le destinataire utilise sa propre clé privée pour déchiffrer le message. « Après avoir établi une session, les clients échangent des messages protégés par une clé de message AES256 en mode CBC pour le chiffrement

et HMAC-SHA256 pour l'authentification. » La session chiffrée doit être recréée uniquement en cas de changement de périphérique ou de réinstallation du logiciel de l'application.

V Autres utilisations de la cryptographie

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 ?) ou encore assurer son intégrité (est-ce qu'il a été modifié ?).

Pour assurer ces usages, la cryptologie regroupe quatre principales fonctions : le hachage avec ou sans clé, la signature numérique et le chiffrement.



a) Pour assurer l'intégrité du message : le hachage

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 ».

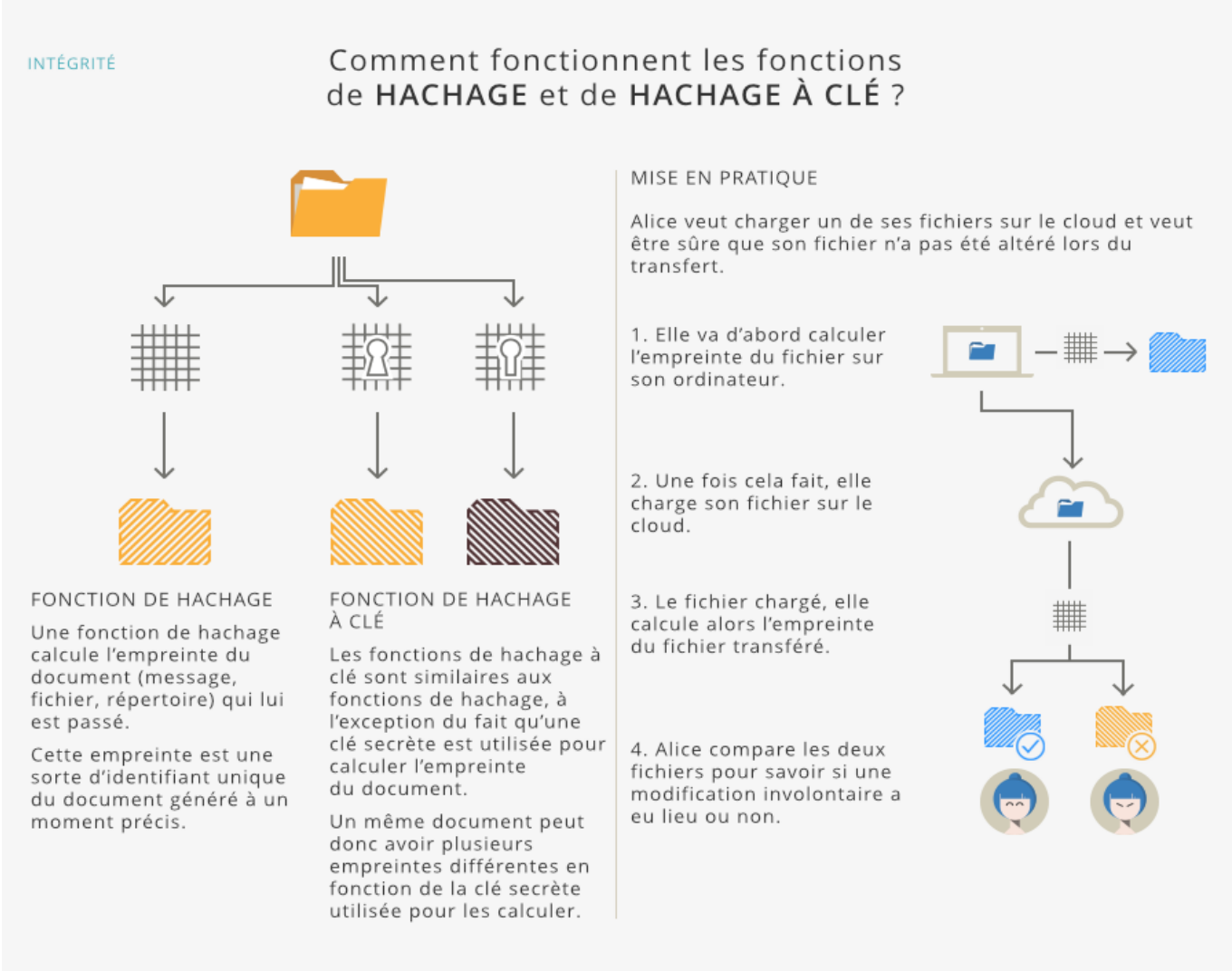
Il ne faut pas confondre le chiffrement, qui permet d'assurer la confidentialité, c'est-à-dire que seules les personnes visées peuvent y avoir accès (voir « Pour assurer la confidentialité du message »), et le hachage qui permet de garantir que le message est intègre, c'est-à-dire qu'il n'a pas été modifié.

Le hachage, pour quoi faire ?
Pour sauvegarder vos photos sur votre espace d'hébergement (de type « cloud » par exemple) et vérifier que votre téléchargement s'est bien déroulé.
Pour synchroniser vos dossiers et détecter ceux qu'il faut sauvegarder à nouveau et ceux qui n'ont pas été modifiés.

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 qu'Alice et Bob calculent la même empreinte, ils doivent tous les deux utiliser la même clé.

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

Le hachage à clé, pour quoi faire ?
- Votre service préféré reconnait votre mot de passe quand vous vous connectez
- Vous voulez pouvoir détecter si quelqu'un modifie des documents sans vous le dire



La communication de données confidentielles par un canal de transmission classique (par exemple Internet) nécessite l'utilisation d'algorithmes de cryptographie classiques : algorithmes de chiffrement asymétrique tels que RSA, ou 748 de chiffrement symétrique (Triple DES, AES).

b) Distribution quantique de clés

Dans le cas du chiffrement symétrique, les deux interlocuteurs doivent posséder a priori une clé secrète, c'est-à-dire qui ne soit connue que d'eux.

Se pose alors la question suivante : comment transmettre une clé de chiffrement entre deux interlocuteurs à distance, à la demande, et avec une sécurité démontrable ? Actuellement, la technique se rapprochant au mieux de ces trois critères est une transmission physiquement sécurisée, de type valise diplomatique.

La cryptographie quantique cherche à répondre à ces trois critères en transmettant de l'information entre les deux interlocuteurs en utilisant des objets quantiques, et en utilisant les lois de la physique quantique et de la théorie de l'information pour détecter tout espionnage de cette information. S'il n'y a pas eu espionnage, une clé parfaitement secrète peut être extraite de la transmission, et celle-ci peut être utilisée dans tout algorithme de chiffrement symétrique afin de transmettre un message.

Pourquoi utiliser le système de cryptographie quantique pour transmettre une clé, et non le message en lui-même ?

Pour deux raisons essentielles :

- Les bits d'informations communiqués par les mécanismes de la cryptographie quantique ne peuvent être qu'aléatoires. Ceci ne convient pas pour un message, mais convient parfaitement bien à une clé secrète, qui doit être aléatoire.
- Même si le mécanisme de la cryptographie quantique garantit que l'espionnage de la communication sera toujours détecté, il est possible que des bits d'informations soient interceptés par l'espion avant que celui-ci ne soit détecté. Ceci est inacceptable pour un message, mais sans importance pour une clé aléatoire qui peut être simplement jetée en cas d'interception.

Paradoxalement, la cryptographie quantique n'est pas de la cryptographie, car elle n'est pas une méthode de chiffrement d'un message utilisant la mécanique quantique. On devrait plus correctement la nommer « distribution quantique de clés », comme c'est bien le cas en anglais (*quantum key distribution*). Il s'agit en effet d'un ensemble de protocoles permettant de distribuer une clé de chiffrement entre deux interlocuteurs distants, tout en assurant la sécurité de la transmission grâce aux lois de la physique quantique et de la théorie de l'information.

Les différents protocoles de cryptographie quantique.

Il existe plusieurs protocoles de cryptographie quantique. On présente souvent celui développé par Bennet et Brassard en 1984, qui utilise la polarisation des photons. On s'y réfère comme le **protocole BB84.**

Le **protocole E91** a lui été imaginé par Artur Ekert en 1991. Il utilise une paire de photons intriqués et donc repose sur l'effet EPR bien mis en évidence par les expériences d'Alain Aspect et ses collègues.

Applications de la cryptographie quantique.

La cryptographie quantique est sortie du domaine de la théorie depuis des années, ce n'est pas une curiosité de laboratoire car elle a déjà été mise en pratique, par exemple et pour la première fois en 2004 pour une importante transaction financière requérant une sécurité absolue et en 2007 lorsque l'entreprise suisse id Quantique a transmis les résultats des élections nationales à Genève.

Bien évidemment, la cryptographie quantique intéresse beaucoup les militaires. La Darpa (agence américaine sur la recherche militaire avancée) utilise ainsi depuis 2004 un réseau de distribution quantique des clefs. L'Union européenne n'est pas en reste car en réponse au programme d'espionnage Echelon, elle a été à l'origine du réseau Secoqc.

Elle ne doit pas être confondue avec la cryptographie post-quantique qui vise à créer des méthodes de cryptographie résistante à un attaquant possédant un calculateur quantique.

Conclusion

La cryptographie n'a cessé d'évoluer pour devenir progressivement une technologie indispensable à notre société moderne d'information, Sans même le savoir nous sommes entourés de moyens cryptographiques, elle est indispensable pour communiquer de façon confidentielle et pour protéger ses données. Comprendre son utilisation permet de réduire les risques de failles de sécurités et de vivre plus sereinement dans une période où les vols de données et d’identités se font de plus en plus nombreux.

Bibliographie

-https://cryptoactu.com/de-la-naissance-de-la-cryptographie-jusqua-la-creation-du-bitcoin/

-Le monde est mathématique : Codage et cryptographie - Mathématiciens, espions et pirates informatiques, de Juan Gomez

-Simon Singh, Histoire des codes secrets, Le Livre de Poche, 2001

-https://www.thawte.fr/assets/documents/guides/history-cryptography.pdf

-http://www.primenumbers.net/Renaud/fr/crypto/index.htm

-https://www.cnil.fr/

-https://www.futura-sciences.com/

-https://www.venafi.com/fr/blog/comment-fonctionnent-les-protocoles-de-chiffrement