EE-TSI	**Cryptographie**	***Cours***

Principes de la cryptographie moderne

Dans la société de l'information d'aujourd'hui, l'usage de la cryptologie s'est banalisé. On le retrouve quotidiennement avec les cartes bleues, téléphones portables, Internet ou encore les titres de transport.

Étymologiquement, la cryptologie est la science (λόγος) du secret (κρυπτός) . Elle réunit:

- _____ (« écriture secrète »)
- _____ (étude des attaques contre les mécanismes de cryptographie).

Les objectifs de la cryptologie sont:

- assurer la _____ (est-on sûre que personne ne lira le message?)
- assurer _____ d'un message (qui a envoyé ce message?)
- assurer _____ du message (le message a-t-il été modifié?)

Pour assurer l'intégrité du message : le hachage

La cryptologie permet de détecter si le message, ou l'information, a été 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. A partir de l'empreinte, on ne peux pas reconstituer l'information de départ.
Cela permet:

- de vérifier que le téléchargement d'un dossier s'est bien déroulé
- de synchroniser des dossier en identifiant ceux qui ont été modifiés
- de stocker les mots de passe de façon sécurisé
- de rechercher aisément une photo spécifique (exemple: Facebook).

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.

Pour assurer la confidentialité du message : le chiffrement

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

Il existe deux grandes familles de chiffrement : le chiffrement symétrique et le chiffrement asymétrique.

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.

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.

Le chiffrement hybride: 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 ».**

Cryptographie à clé publique

Commençons par expliquer ceci de façon imagée. Un ami doit vous faire parvenir un message très important par la poste, mais vous n'avez pas confiance en votre facteur que vous soupçonnez d'ouvrir vos lettres. Comment être sûr de recevoir ce message sans qu'il soit lu? Vous commencez par envoyer à votre ami un cadenas sans sa clé, mais en position ouverte. Celui-ci glisse alors le message dans une boite qu'il ferme à l'aide du cadenas, puis il vous envoie cette boite. Le facteur ne peut pas ouvrir cette boite, puisque seul vous, qui possédez la clé, pouvez le faire.

La cryptographie à clé publique repose exactement sur ce principe. On dispose d'une fonction P qui permet de chiffrer les messages. Ce procédé est inversible, c'est-à-dire que l'on dispose d'une fonction de déchiffrement S. On peut fabriquer simultanément un couple (P,S), mais connaissant uniquement P, il est impossible (ou au moins très difficile) de retrouver S.

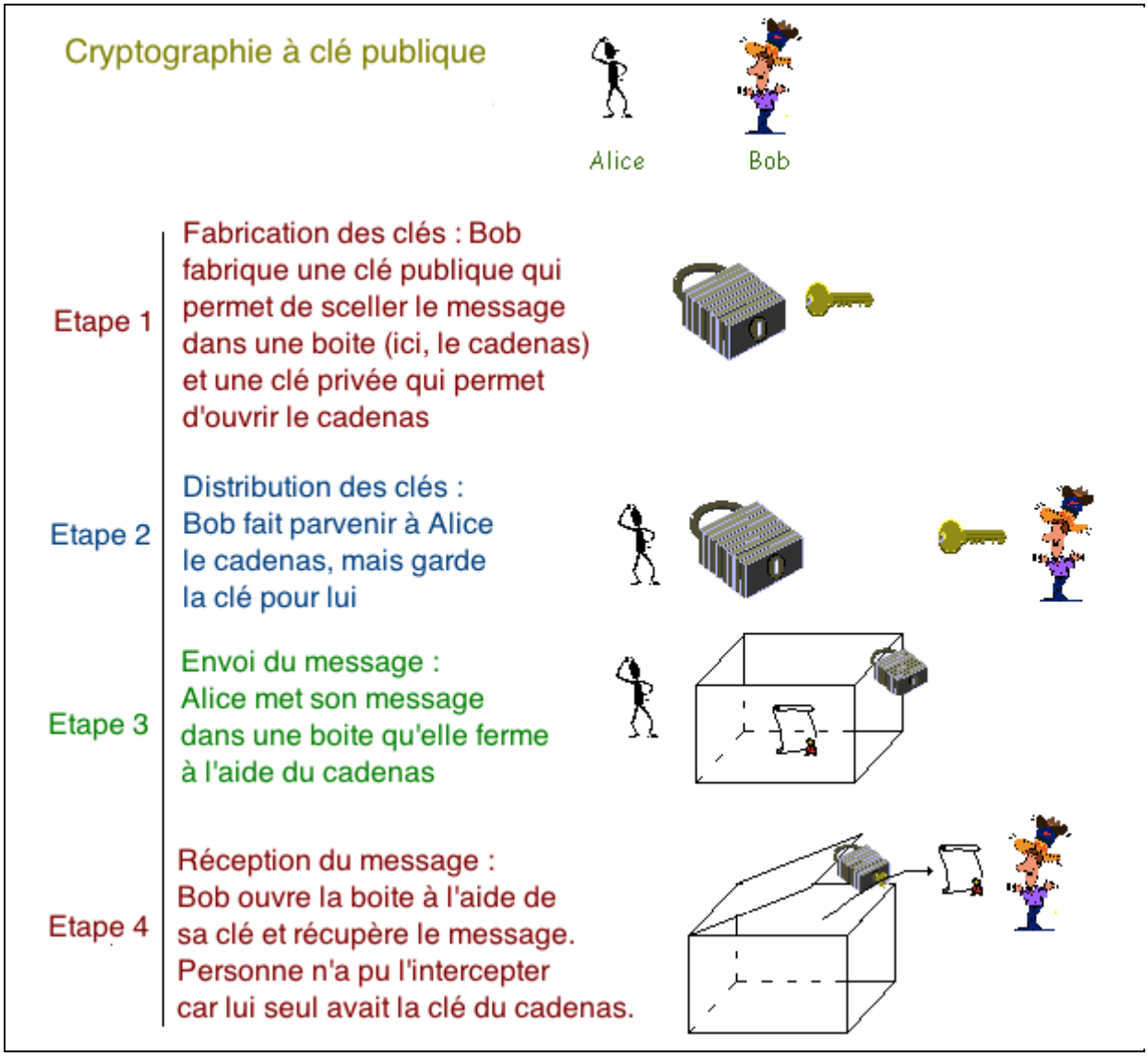
- P est la **clé publique** (le cadenas), que vous pouvez révéler à quiconque. Si quelqu'un veut vous envoyer un message, il vous transmet P(message).

- S est la **clé secrète** (la clé du cadenas), elle reste en votre seule possession. Vous décodez le message en calculant S(P(message))=message.
- La connaissance de P par un tiers ne compromet pas la sécurité de l'envoi des messages codés, puisqu'elle ne permet pas de retrouver S. Il est possible de donner librement P, qui mérite bien son nom de clé publique.

Comment trouver de telles fonctions P et S?

- il est facile de fabriquer de grands nombres premiers p et q (pour fixer les idées, 500 chiffres).
- étant donné un nombre entier n=p.q produit de 2 grands nombres premiers, il est très difficile de retrouver les facteurs p et q.

La donnée de n est la clé publique : elle suffit pour chiffrer. Pour déchiffrer, il faut connaitre p et q, qui constituent la clé privée. Le problème de factorisation de grands entiers étant très difficile, la connaissance de la clé publique n ne permet pas de retrouver les entiers p et q, qui constituent la clé secrète.



Le talon d'Achille de la crypto

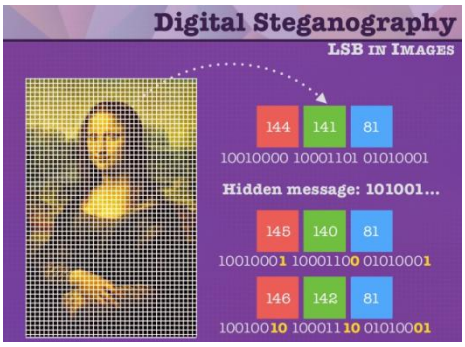
En fait le talon d'Achille des solutions existantes de cryptographie est le processus d'échange des clefs. Tandis que les techniques conventionnelles de distribution se fondent sur la clef publique ou l'échange manuel. Une entité qui « renifle » le flux peut donc intercepter l'échange de clef, générer une fausse clef et se faire passer pour l'entité émettrice. Le récepteur va donc coder son message avec la fausse clef ce qui aura pour conséquence, primo que le message sera décodé par l'intrus en temps réel, et deuxio que le destinataire ne recevra pas le message d'origine, mais éventuellement un message modifié…

La STEGANOGRAPHIE : dissimuler l'information au lieu de la crypter

La steganographie a été inventée par les Grecs pour dissimuler des informations à leurs ennemis. Ils inscrivaient sur le crane d'un esclave une information sensible, les cheveux repoussaient, puis le moment venu ils envoyaient l'esclave à leur allié. Le message était récupéré en rasant la tête de l'esclave.

Le mot steganographie vient du Grec « steganos » qui veut dire « caché » mais dans le sens de « enfoui », comme un sous-marin... Le mot Grec « crypto » veut dire également « caché », mais dans le sens « on ne comprend pas la signification ». Deux mots de Grec donc, pour deux traitements des informations sensibles, distincts et complémentaires.

La steganographie moderne utilise un programme qui va encapsuler le fichier secret à protéger dans un autre fichier dit « hôte », plus grand, et qui sera anodin comme une photo ou une musique. Ce qui rend le fichier secret totalement invisible et perdu dans la masse de fichiers « en clair »…



La CRYPTO Quantique

Les équipements cryptographiques quantiques utilisent des photons de lumière polarisés et tirent profit du principe de Heisenberg: la mesure d'un système quantique modifie l'état du système qu'il cherche à mesurer.

L'émetteur transmet au récepteur une chaîne continue de bits véhiculés par des grains de lumière appelés photons. Si un intrus essaie de les intercepter, leur état changera de manière irréparable. L'émetteur et le récepteur détecteront la tentative d'espionnage. La chaîne corrompue est alors rejetée et ne sera pas utilisée pour établir une clé. Seuls les photons intègres fournissant une information sans risque participent à la génération de clés secrètes.