Partie 1

Chiffrements asymétriques

Le chiffrement symétrique permet de communiquer de manière *confidentielle*, ou de préserver la *confidentialité* de nos données sur un disque dur.

Le problème avec le seul chiffrement symétrique, c'est qu'il ne permet pas de repondre aux besoins d'*authentification* (reconnaitre l'identité) et d'*authenticité* (le message n'a pas été modifié).

Pour comprendre ces termes, on utilise le scenario suivant. Alice et Bob sont 2 personnes qui veulent echanger des messages de manière sécurisée. Une 3e personne, appelée *Trudy*, ou Eve, joue le rôle d'un attaquant.

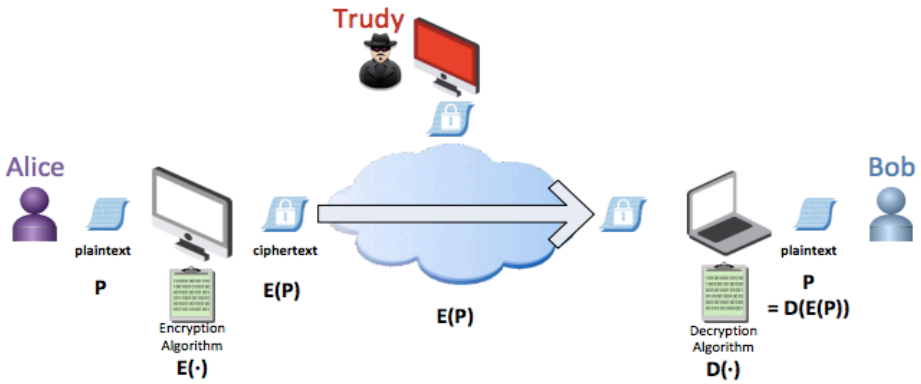

FIGURE 1 – Le trio Alice - Bob - Trudy

Le chiffrement asymétrique utilise plusieurs clés, une pour le ....., et une autre pour le .....
Il repose sur des propriétés mathématiques de l'arithmetique modulaire. (voir principe du chiffrement RSA)

> Complément sur RSA (Grand Oral)

Lors de la confection de la clé publique `e`*, le propietaire de la clé utilise la valeur de 2 entiers* `p` *et* `q` *premiers entre eux (secrets). La clé privée* `d` *est alors calculée comme inverse modulaire de* `e` *(modulo* $(p-1).(q-1)$*).*

Pour chiffrer le caractère de valeur numérique M on fait : $M^e(mod\ n)$ *et pour dechiffrer :* $M^d(modn)$ *ou* `n=p.q`

On exploite la propiété qui veut que $(M^e)^d = M(mod\ n)$

Or, casser la clé revient à rechercher l'inverse modulaire de `e`*, ce qui est impossible sans connaitre* `p` *et* `q`*, du moins en un temps limité. Et avec les algorithmes classiques, casser la factorisation croit exponentiellement avec la longueur de la clé.*

1.1 Principe du chiffrement RSA

1.1.1 Confidentialité

Il doit y avoir 2 clés. L'une de ces clés doit rester secrête, et conservée par l'expediteur du message : c'est la clé **privée**. L'autre clé utile pour le chiffrement et le dechiffrement est partagée : elle est dite **publique**. On peut indifféremment chiffrer avec la clé publique et déchiffrer avec celle privée, ou l'inverse.

Ainsi, comme la clé de Bob est publique, Alice peut utiliser cette clé pour chiffrer le message qu'elle veut lui envoyer, un peu comme si elle mettait le message dans un coffre (*celui de Bob*). Et Bob, qui possède la clé privée

correspondante (la clé de *son* coffre) peut alors déchiffrer le message d'Alice.

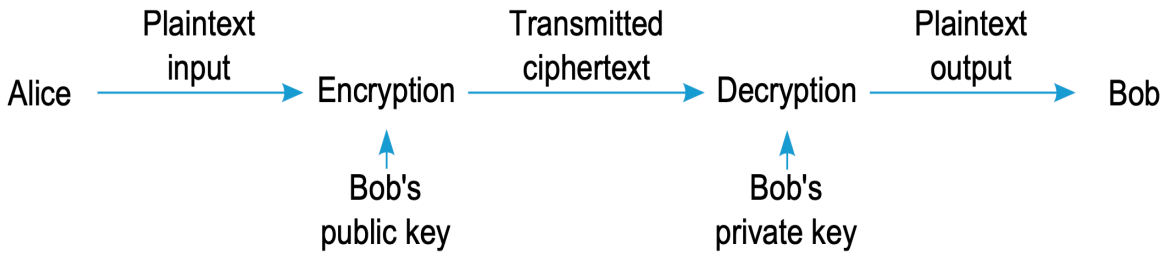

FIGURE 2 – Chiffrement asymetrique

1.1.2 Authentification

On peut utiliser cet algorithme pour authentifier l'auteur du message, et réaliser une **signature numérique**.

Imaginons que Bob utilise sa clé *privée* pour chiffrer un message M. Il l'envoie à Alice, qui, en utilisant la clé publique de Bob, pourra le déchiffrer. Elle pourra ainsi s'assurer que Bob en est bien à l'origine et que son contenu n'a pas été modifié.

En effet, comme il est le seul à posséder la clé *privée*, ce message M vient bien de Bob.

> Compléter la situation où Bob envoie un message de type Bonjour à Alice, en utilisant sa clé privée :

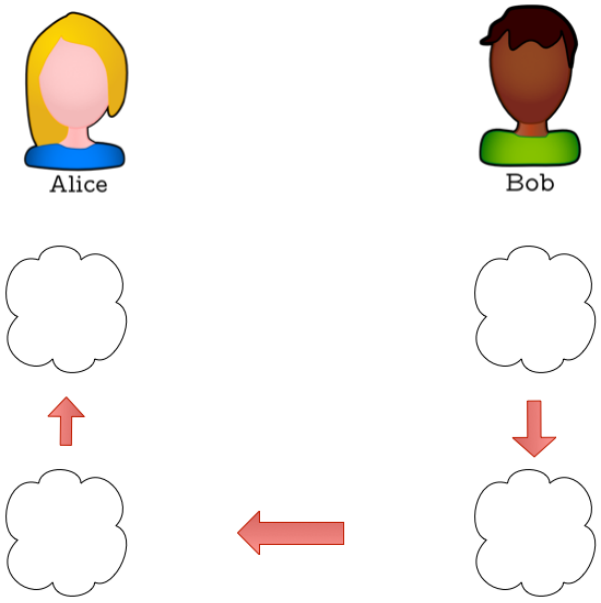

FIGURE 3 – Bonjour Alice - via chiffrement asymetrique

Le point faible de cet échange vient de la distribution de la clé publique entre Bob et Alice.

Cet échange n'est réellement sécurisé qu'à la condition que la clé publique de Bob, vienne bien de Bob. Et que personne ne se soit introduit dans la discussion pour substituer la clé publique de Bob par la sienne (attaque de l'*homme du milieu*).

> Compléter la situation suivante où Eve réalise une attaque dite de l'homme du milieu. Elle envoie au préalable sa propre clé publique à Alice et Bob. Puis elle se fait passer pour chacun des 2 lors de la discussion.

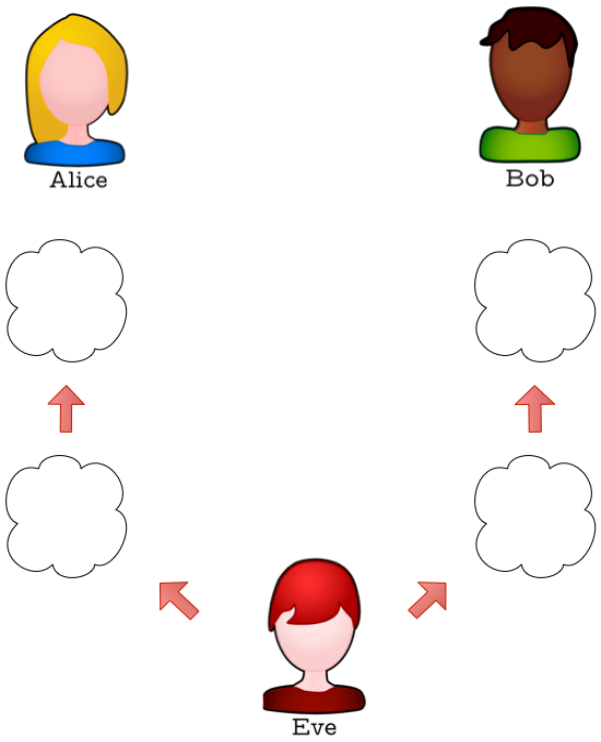

FIGURE 4 – Bonjour Alice, bonjour Bob - Eve

Pour s'authentifier, Bob doit d'abord envoyer à Alice un *certificat*, qui contient sa clé publique mais aussi d'autres informations qui permettent de verifier la validité de ce certificat, en particulier l'*emetteur* : le nom de l'autorité de certification, une *infrastructure à clé publique* (PKI) qui a validé l'identité de Bob.

Certificats : les navigateurs font confiance à certaines autorités de certification, qui ont au préalable, certifié leurs clients (possesseurs de sites web).

Si la chaine de confiance est rompue, votre navigateur vous en informe.

En pratique, le certificat est un ensemble d'informations sur le propriétaire du domaine, la durée de validité, l'algorithme utilisé pour l'authentification, la clé publique, et surtout l'*emetteur*. Lorsqu'Alice reçoit le certificat que lui envoie Bob, elle consulte l'*emetteur* du certificat pour verifier qu'il s'agit bien du bon certificat, que celui-ci appartient bien à Bob.

Partie 2

Principe d'une communication securisée HTTPS

Lors d'une communication HTTPS : les objectifs d'authentification, authenticité et de confidentialité sont remplis. Lors du protocole de communication, les chiffrements asymétriques et symétriques sont tous 2 utilisés :

- le client demande au serveur que celui-ci s'authentifie (1) et (2)
- le client envoie de manière sécurisée une clé de session qui servira pour la communication (3). L'envoie de la clé se fait à l'aide du chiffrement asymétrique. Le client utilise la clé publique du serveur pour cet envoi.
- Cette clé sera utilisée pour des chiffrements symétriques (4).

FIGURE 5 – établissement d'une communication securisée - OVH

Partie 3

Exercices

3.1 Nombre de clés :

Un groupe de n personnes souhaitent communiquer entre elles, chacune, deux à deux. Elles souhaitent utiliser un moyen de communication sécurisé par un chiffrement symétrique. Combien de clés différentes seront nécessaires ?

3.2 Méthode de chiffrement de Vigenère.

Si on appliquait cette méthode à un alphabet de 95 caractères (les caractères ascii) :

1. Combien de clés différentes peuvent exister avec 4 caractères ?
2. Combien de temps cela prendrait-il au maximum pour déchiffrer un message par recherche exhaustive (force brute), si le temps de calcul pour le déchiffrement est de 1 milliseconde par clé ?

3.3 Mots de passe

1. Combien de mots de passe différents de 10 caractères peuvent être générés à l'aide des 95 caractères ascii ?

2. Avec un ordinateur capable de tester 1 million de mots de passe par seconde, combien de temps cela lui prendra t-il pour explorer l'ensemble des combinaisons ?
3. Expliquer ce qu'est une attaque par recherche exhaustive.
4. Pour les proriétaires d'un site internet, vaut-il mieux conserver dans la base de données, les mots de passe des clients, ou bien le hachage de chacun de ces mots de passe ?

3.4 RSA

1. Quel est la valeur de 8^7 modulo 40 ?
2. Verifier que 55 est decomposable en produit de 2 nombres premiers p et q. Calculer `(p-1)*(q-1)`
3. Soit la clé publique $e = 3$. Quel est l'inverse de e modulo 40 ? Appeler ce nombre d.
4. Chiffrer le message M = 5 avec la clé publique `e`, selon $M^e (mod\ 55)$
5. Dechiffrer $M^e (mod\ 55)$ avec la clé privée `d`, selon la même fonction que précédemment.
6. Dans un protocole de chiffement asymétrique, les algorithmes de chiffrement et de déchiffrement sont-ils les mêmes ?
7. Dans un protocole de chiffrement asymétrique, toutes les personnes possédant la clé publique de Bob peuvent lui envoyer un message ?
8. Dans un protocole d'authentification, toutes les personnes possédant la clé publique de Bob peuvent vérifier sa signature émise ?
9. Supposons que Bob envoie à Alice un message chiffré de la manière suivante : `C = chiffrement(m, Bob_public_key)`. Est-ce qu'Alice peut authentifier Bob avec ce message ?
10. Supposons que Bob envoie à Alice un message chiffré de la manière suivante : `C = chiffrement(m, Bob_private_key)`. Est-ce que ce message est confidentiel ?