Le chiffrement

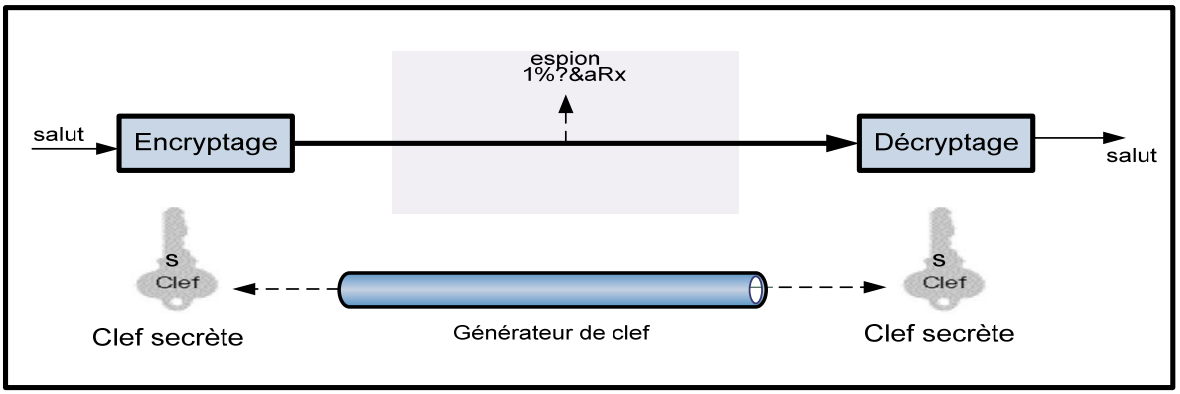
Un chiffrement moderne permet d'assurer :

- La **Confidentialité** des informations
- L'**Intégrité** des données en s'assurant que l'information n'a pas subi de modification
- **l'authentification** afin de vérifier que le message correspond bien à l'expéditeur.

Avant d'aborder les techniques modernes de chiffrement sur les réseaux nous allons rappeler les différents principes de chiffrement : le chiffrement symétrique, asymétrique ou mixte.

Cryptographie à clé secrète (chiffrement symétrique)

On utilise une clef secrète commune aux 2 systèmes qui veulent communiquer ensemble.
Les algorithmes symétriques actuels sont nettement plus rapides que les algorithmes asymétriques. Une clef symétrique est toutefois potentiellement peu sûre. Il suffit qu'un individu malintentionné se procure la clé secrète et il n'y a plus d'information protégée. La clef symétrique doit donc être transmise au correspondant sans être interceptée.



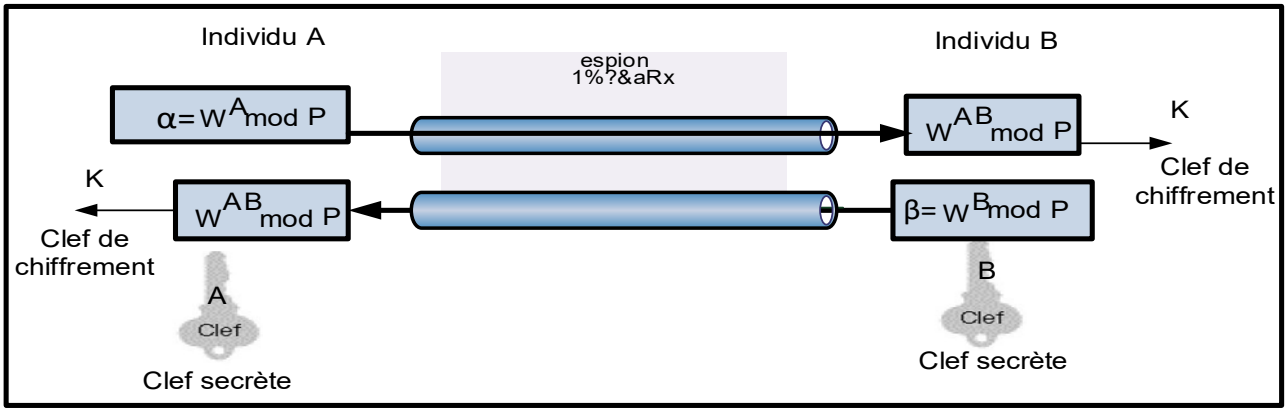
Les algorithmes de cryptage symétriques les plus répandus sont le **DES et le 3DES.**

La vulnérabilité de la cryptographie symétrique repose sur l'échange de clé.
Diffie et Hellman ont proposé une méthode afin de convenir d'un secret partagé sans le faire circuler entre les participants, en d'autres termes une fonction mathématique telle que les participants puissent échanger des informations dont eux seuls pourraient déduire le secret.

Le protocole repose sur la fonction suivante :

$$K = w^{A \times B} mod\ P$$

Cette fonction est publique, ainsi que les valeurs de W et P

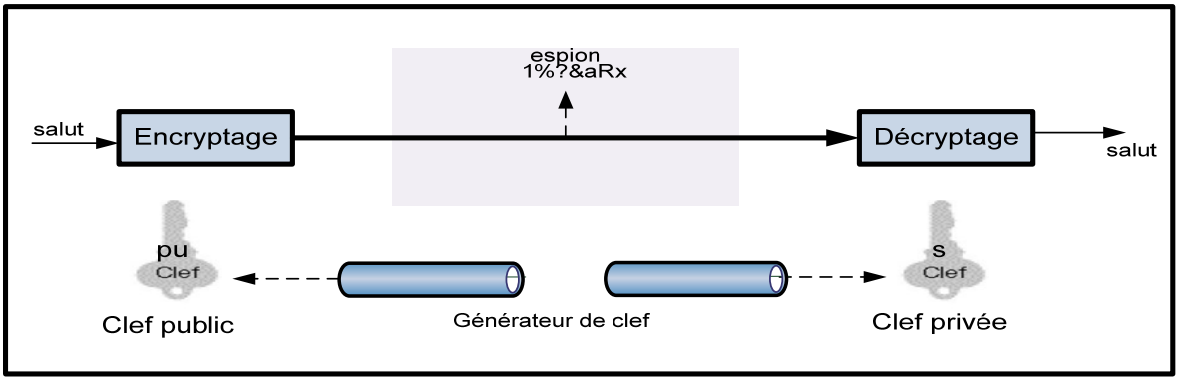


Chaque individu A et B dispose de sa propre clé secrète respectivement A et B. Chacun individu envoi une partie du message β et a sans directement transmettre A et B mais qui permet à A ou B de trouver la clé secrète K.

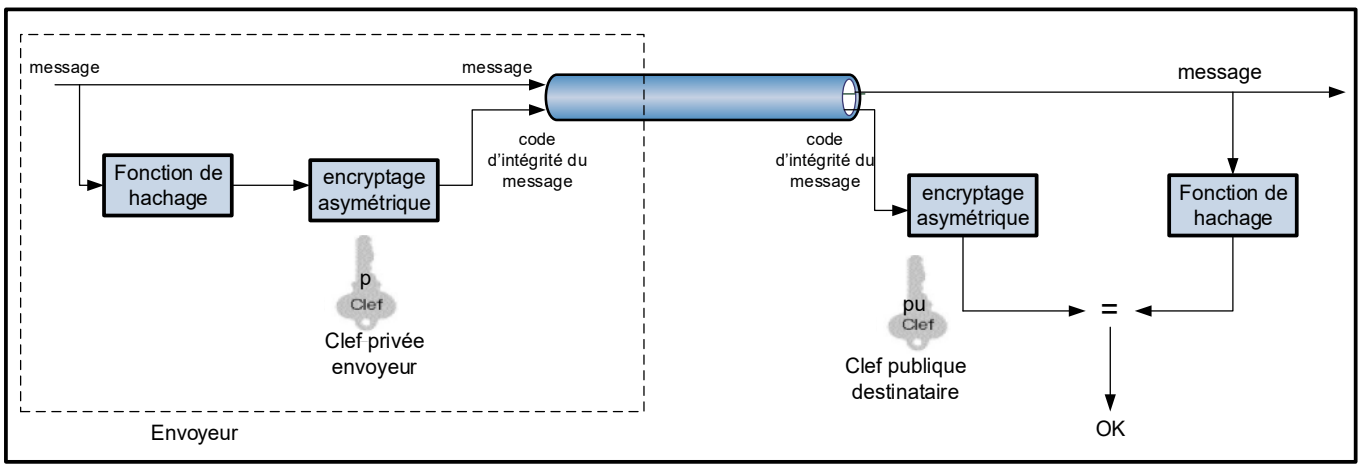
La clé K n'a jamais été directement transmise et il est très difficile à un espion de trouver la clé K connaissant que β et a. Le système reste fiable si P a un format de 512 octets.

Cryptographie à clé publique (chiffrement asymétrique)

Le chiffrement à base de clef publique garantit qu'une donnée chiffrée par une clef, **publique ou privée**, ne peut être déchiffrée que par la clef associée. Les clefs sont de même nature et leurs rôles peuvent être inversés : ce que l'un chiffre est déchiffrable par l'autre. La paire de clef repose sur des nombres premiers.
L'astuce consiste à conserver une clef secrète (la clef privée) et à distribuer l'autre clef (la clef publique) à tout le monde. N'importe qui peut vous envoyer un message chiffré mais personne d'autre que vous ne peut le déchiffrer tant que vous êtes le seul à conserver un des deux membres de la paire de clefs.



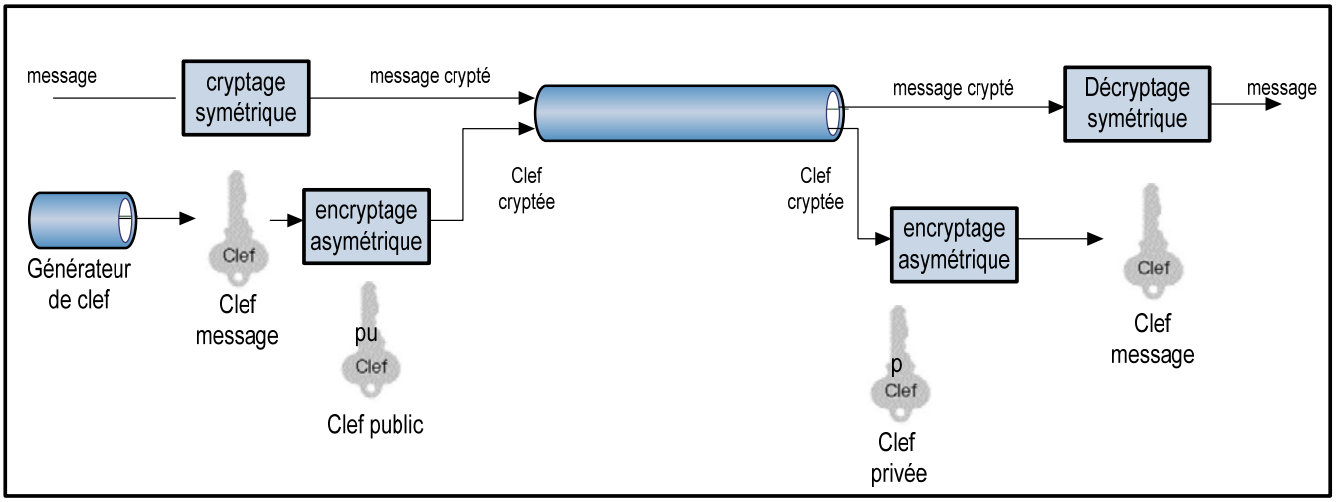
La signature d'un message consiste à associer une identité à son contenu. L'identité du message est représentée par une suite binaire que l'on appelle le checksum. On applique le message à l'entrée d'une fonction de hachage qui fournit en sortie un résultat appelé haché. Le haché est ensuite crypté par la clef privée. Le destinataire de l'ensemble (message + code d'intégrité) recalcule le haché et le compare au résultat du déchiffrement de la signature ou code d'intégrité avec la clef publique.



La caractéristique principale d'une fonction de hachage est de produire un haché des données, c'est-à-dire un condensé de ces données.

La solution mixte

On utilise un système asymétrique (comme **RSA** ou **Diffie-Hellman**) pour crypter les clés de Message. Ces clés de message permettront de chiffrer le message grâce à un chiffrement symétrique (DES, 3DES, IDEA, RC4...).



Le problème du chiffrement asymétrique vient de la transmission de la clé publique. Si celle-ci n'est pas sécurisée, une personne malveillante peut se positionner entre l'entité et son public en diffusant de fausses clés publiques (par le biais d'un faux site internet par exemple) puis intercepter toutes les communications, lui permettant d'usurper l'identité du diffuseur de clés publique.
Pour un chiffrement asymétrique le passage de clé s'effectue par un certificat. Plus précisément, un certificat est une structure de données contenant une clé publique, des informations sur le propriétaire du certificat, l'ensemble étant signé par une autorité tierce appelée *Autorité de Certification (AC,ou Certificate Authority : CA).*
Le format de certificats le plus utilisé dans le cadre d'une *PKI (Public Key Infrastructure ou IGC)* est X.509v3. Ce dernier permet l'utilisation des protocoles normalisés tels que SSL ou encore IPSec.

Un certificat numérique contient les informations suivantes :

- La *clé cryptographique publique* de la paire de clés du sujet du certificat.
- Des *informations sur le sujet* qui a demandé le certificat.
- Des *informations sur l'Autorité de certification* qui a émis le certificat.

Avant d'émettre un certificat, l'Autorité de certification vérifie l'identité du demandeur. Cette vérification peut inclure une enquête de fond manuelle du demandeur ou un examen de la liste de contrôle d'accès discrétionnaire (DACL, *Discretionary Access Control List*) du modèle de certificat demandé, et ce pour garantir que l'utilisateur ou l'ordinateur à l'origine de la demande dispose des autorisations nécessaires pour inscrire le certificat demandé.

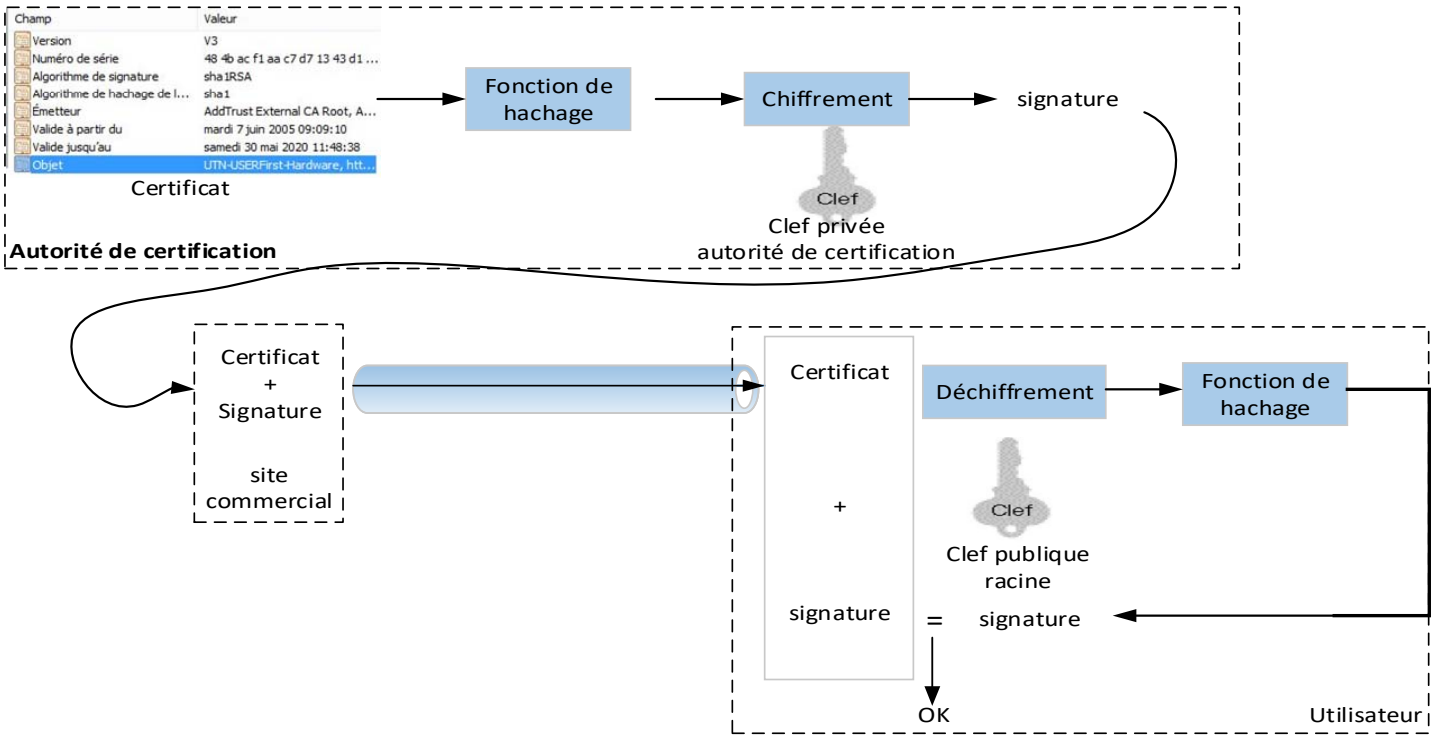
Champ	Valeur
Version	V3
Numéro de série	48 4b ac f1 aa c7 d7 13 43 d1 ...
Algorithme de signature	sha1RSA
Algorithme de hachage de l...	sha1
Émetteur	AddTrust External CA Root, A...
Valide à partir du	mardi 7 juin 2005 09:09:10
Valide jusqu'au	samedi 30 mai 2020 11:48:38
Objet	UTN-USERFirst-Hardware, htt...

Champ	Valeur
Clé publique	RSA (2048 Bits)
Identificateur de clé de l'aut...	ID de la clé=ad bd 98 7a 34 b...
Identificateur de la clé du s...	a1 72 5f 26 1b 28 98 43 95 5d...
Points de distribution de la li...	[1]Point de distribution de la lis...
Utilisation de la clé	Signature du certificat, Signat...
Contraintes de base	Type d'objet=Autorité de certi...
Algorithme d'empreinte num...	sha1
Empreinte numérique	3d 4b 2a 4c 64 31 71 43 f5 02 ...

Les champs de base sont les suivants :

- **Version :** indique à quelle version de X509 correspond ce certificat.
- **Numéro de série :** Numéro de série du certificat.
- **Algorithme de signature :** identifiant du type de signature utilisée.
- **Emetteur :** DN de l'autorité de certification qui a émis ce certificat.
- **Valide à partir de :** la date de début de validité de certificat.
- **Valide jusqu'à :** la date de fin de validité de certificat.
- **Objet :** Distinguished Name (DN) de l'objet de ce certificat.
- **Clé publique de l'objet :** infos et clé publique de ce certificat.

La création d'un certificat et son identification s'effectue de la façon suivante:



Les autorités de certification sont des organismes enregistrés et certifiés auprès d'autorités publiques ou de gouvernance de l'internet qui établissent leur viabilité comme intermédiaire fiable. Ces organismes diffusent leurs propres clés publiques. Étant certifiées fiables ces autorités sont en contact direct avec les principaux producteurs de système d'exploitation et de navigateurs internet (tels que Mozilla Firefox, Internet Explorer, Google Chrome...) qui incluent nativement les listes de clés des autorités de certification. Ces clés sont appelées ***clés***

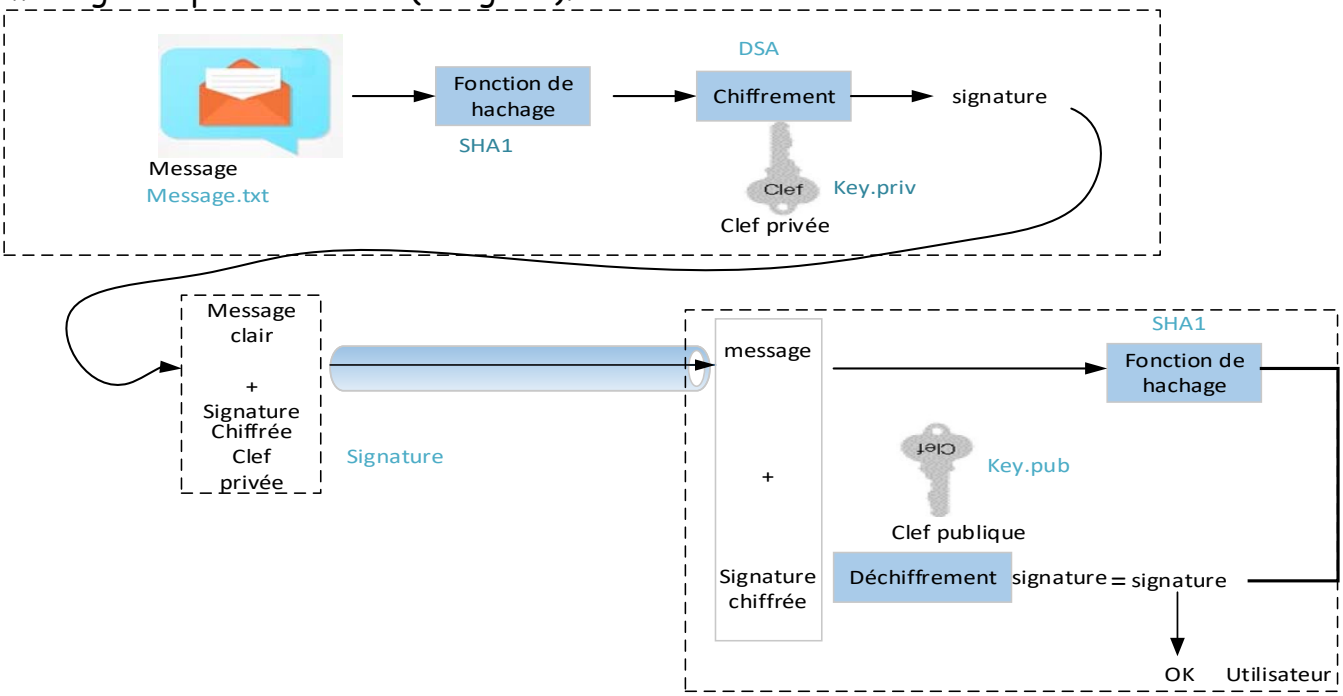
publiques racines ou *clé root*, elles sont utilisées pour identifier les clés publiques d'autres organismes.

Lorsqu'un site commercial veut diffuser une clé publique dans un certificat, il contacte une autorité de certification. Celle-ci va recevoir la clé publique et l'identité du diffuseur. Après avoir vérifié l'identité du demandeur par des moyens conventionnels, l'autorité de certification place l'identité et la clé publique fournie dans un conteneur qu'elle signe en utilisant sa clé privée. Le fichier résultant est le certificat. Il est rendu au diffuseur ou au site commercial.

Le site commercial utilise le certificat pour ses communications (par exemple sur son site internet): un utilisateur reçoit le certificat, il le vérifie avec la **clé racine publique** de l'organisme de certification incluse dans son navigateur. Le déchiffrement authentifie le contenu du certificat et prouve que la clé publique et l'identité contenus dans le certificat sont certifiés liés par l'autorité de certification. L'utilisateur sait donc qu'il pourra récupérer les informations envoyées en utilisant la clé publique et qu'elles ne seront pas interceptées par un tiers.

La signature numérique

Pour signer le message envoyé, on procède de la façon suivante : l'expéditeur applique au message clair une fonction mathématique (appelée fonction de hachage) qui produit un "résumé" (code haché) du message. Le résumé obtenu est propre à chaque message, à l'image d'une empreinte digitale. Le code haché peut ensuite être chiffré à l'aide de la clé privée de l'expéditeur et être annexé au message envoyé. C'est ce code qui constitue la signature numérique. Le destinataire du message peut ensuite vérifier que l'expéditeur est bien le bon en déchiffrant la signature numérique, au moyen de la clé publique correspondante, pour obtenir le code haché. Le destinataire applique ensuite la même fonction de hachage au message reçu ; si les deux codes sont identiques, l'expéditeur du message est bien le bon (non-répudiation) et le message n'a pas été altéré (intégrité).



Il existe plusieurs algorithmes proposant des fonctions de hachage. Les principaux sont :

MD4 et MD5 (Message Digest). MD5 produit des hachés de 128 bits en travaillant les données originales par blocs de 512 bits.

SHA-1 (Secure Hash Algorithm 1) ; comme MD5, il est basé sur MD4. Il fonctionne également à partir de blocs de 512 bits de données et produit par contre des condensés de 160 bits en sortie. Il nécessite donc plus de ressources que MD5.

SHA-2 (Secure Hash Algorithm 2) qui a été publié récemment et est destiné à remplacer SHA-1. Les différences principales résident dans les tailles de hachés possibles : 256, 384 ou 512 bits. Il sera vraisemblablement bientôt la nouvelle référence en terme de fonction de hachage.

Principe SSH

SSH est un moyen de connexion en ligne de commande crypté de la couche 7 du modèle OSI
SSH utilise le principe de clé asymétrique RSA (Clé privée + clé publique) pour créer une clé de session de cryptage (DES en SSH-1), principe du chiffrement mixte
La clé publique peut être librement publiée tandis que la clef privée doit rester secrète. La connaissance de la clef publique ne permet pas d'en déduire la clé privée.
Le serveur SSH (dans notre cas le switch) dispose du couple de clefs RSA stocké et généré lors de l'installation du serveur (sans certificat en SSH-1)

1/ Connexion Client

2/ Envoi clé publique du serveur au client (Vérification "fingerprint" éventuelle la première fois pour éviter un faux serveur)

3/ Génération puis crytage d'une clé de session avec clé publique

4/ Envoi clé de session cryptée au serveur

5/ Décryptage clé de session par clé privée (ce qui prouve que c'est le bon client !)

6/ Envoi d'un message du serveur crypté avec clé de session puis décryptage par le client avec la même clé (ce qui prouve que c'est le bon serveur :)

6/ Authentification du client finale en login/mot de passe

