Objectifs atteints lors d'une communication chiffrée par ssh

	Authentification	Confidentialité	Intégrité
Step 1			
Step 2	✔		
Step 3			
Step 4	✔	✔	✔
Step 5		✔	✔

Par mot de passe (steps 1 to 5):
$ ssh moi@srv.tux.be
Password :
$ ls -l

Par clef (steps 1 to 5):
$ ssh moi@srv.tux.be
$ ls -l

La ***non-répudiation*** n'est pas un objectif atteint par ssh car la distribution de la clé publique n'est pas toujours sûre.

CLIENT SERVEUR

S1 Négociation

. Se mettent d'accord sur les crypto-systèmes à utiliser par la suite et la version du protocole ssh à utiliser (ex. ssh2)
Ex. RSA pour le chiffrement asymétrique
AES pour le chiffrement symétrique
SHA pour le hachage

. $Kpub_S$ ◄ - $Kpub_S$ / $Kpriv_S$

S2 Authentification du serveur
(Le serveur doit répondre à un défi)

Création d'un challenge

7+5 RSA - RSA → 7+5
$Kpub_S$ $Kpriv_S$

✔ 12 ◄ - 12

ASYMETRIQUE

S3 Ouverture d'un canal sécurisé

. Echange sécurisé d'une clé de session (Diffie-Hellman)
Kses ◄ - Kses

. Les data qui seront échangées par la suite passeront par un canal ssh
→ AES - AES →
Kses Kses

S4 Authentification du client

(Soit 'jean' qui veut se connecter)

. Par MDP
login/pwd → AES - AES →
Kses + SHA Kses

SYMETRIQUE

. Par CLE
'jean' aura généré au préalable un trousseau côté client ($Kpub_{jean}$ / $Kpriv_{jean}$) et sa clé publique est recopié dans sa home directory côté serveur.

Le client doit répondre à un défi

Création d'un challenge

8+7 ← RSA ◄ - RSA ← 8+7
$Kpriv_{jean}$ $Kpub_{jean}$

15 - 15 ✔

ASYMETRIQUE

S5 Communication

La communication peut alors débuter et passe par le canal ssh créé en step3

Data → AES - AES → Data
Kses + SHA Kses

SYMETRIQUE