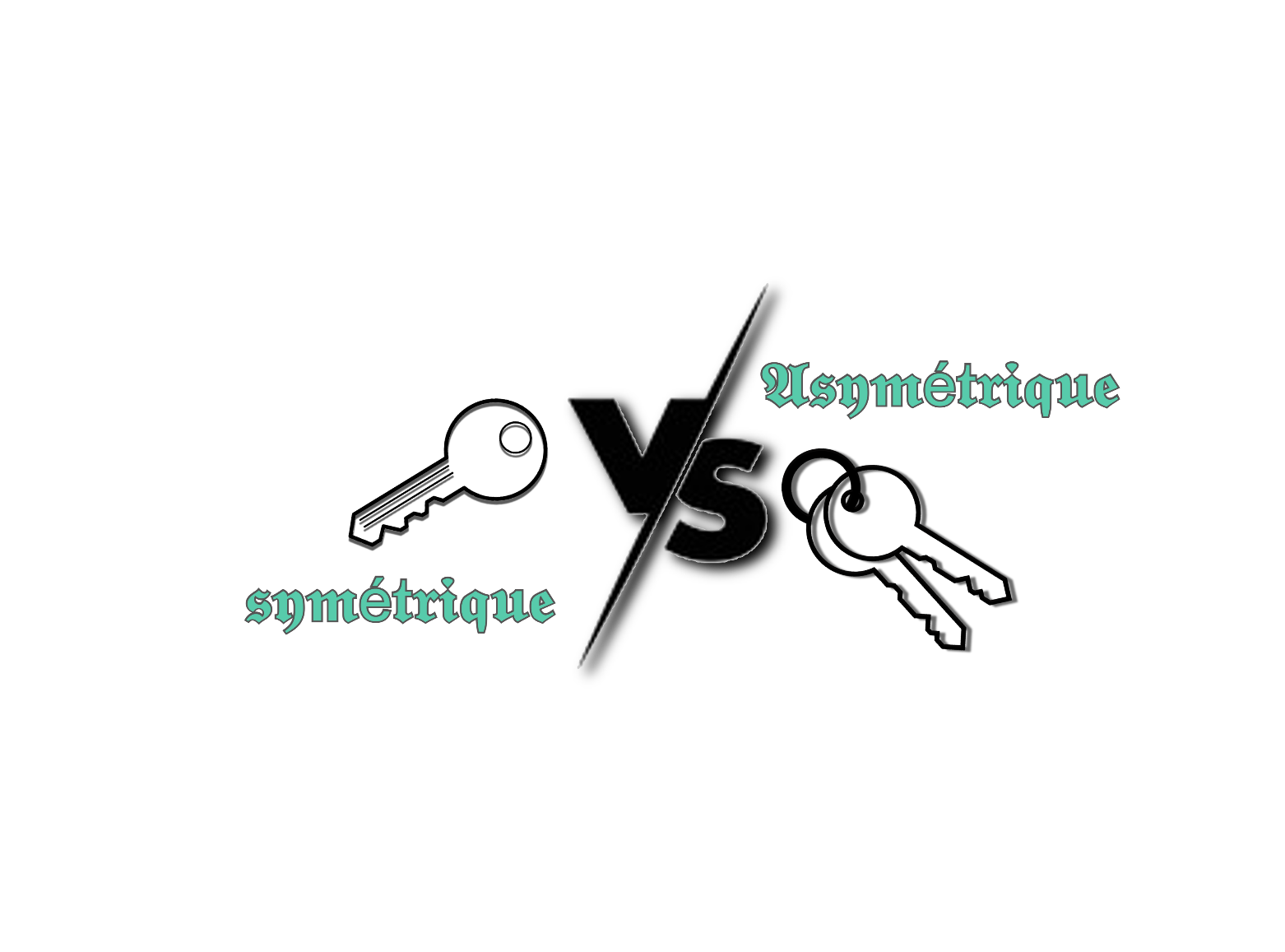
**Compte rendu**

**Semaine 17**



Réalisé par : Encadré par :

🌢 OTHMANE TAYBI 🌢 Mr. A.OMOR

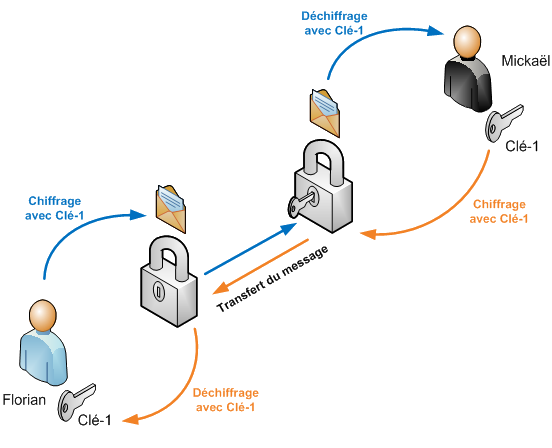
CRYPTAGE SYMETRIQUE

VS

CRYPTAGE ASYMETRIQUE :

**🗹Cryptage symétrique :**

**🕉** Les algorithmes de chiffrement symétrique se fondent sur une même clé pour chiffrer et déchiffrer un message. L’un des problèmes de cette technique est que la clé, qui doit rester totalement confidentielle, doit être transmise au correspondant de façon sûre**.** La mise en œuvre peut s’avérer difficile, surtout avec un grand nombre de correspondants car il faut autant de clés que de correspondants.



**🕉 Quelques algorithmes de chiffrement symétrique très utilisés**

🄌Chiffre de Vernam (le seul offrant une sécurité théorique absolue, à condition que la clé ait au moins la même longueur que le message, qu’elle ne soit utilisée qu’une seule fois à chiffrer et qu’elle soit totalement aléatoire)

➊DES

➋3DES

➌AES

➍RC4

➎RC5

➏MISTY1

➐Et bien d’autres.

**🕉 Quelque exemple de chiffrement symétrique :**

****

****

**🗹Cryptage Asymétrique :**

**🕉** Pour résoudre le problème de l’échange de clés, la cryptographie asymétrique a été mise au point dans les années 1970. Elle se base sur le principe de deux clés :

🌢 Une publique, permettant le chiffrement.

🌢 Une privée, permettant le déchiffrement.

**✠** Comme son nom l’indique, la clé publique est mise à la disposition de quiconque désire chiffrer un message. Ce dernier ne pourra être déchiffré qu’avec la clé privée, qui doit rester confidentielle.

**✠** Ceci dit le rôle des clés est interchangeable : on peut chiffrer avec une clé privée et déchiffrer avec une clé publique.

**✠** Quelques algorithmes de cryptographie asymétrique très utilisés :

🌢 RSA (chiffrement et signature).

🌢 DSA (signature).

🌢 Protocole d’échange de clés Diffue-Hellman (échange de clé).

🌢 Et d’autres ; voir cette liste plus complète d’algorithmes de cryptographie asymétrique.

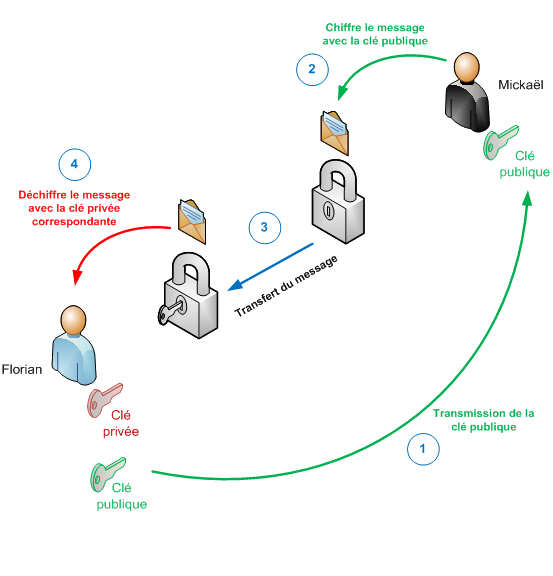
**✠** Le principal inconvénient de RSA et des autres algorithmes à clés publiques est leur grande lenteur par rapport aux algorithmes à clés secrètes. RSA est par exemple 1000 fois plus lent que DES. En pratique, dans le cadre de la confidentialité, on s’en sert pour chiffrer un nombre aléatoire qui sert ensuite de clé secrète pour un algorithme de chiffrement symétrique. C’est le principe qu’utilisent des logiciels comme PGP par exemple.

**✠** La cryptographie asymétrique est également utilisée pour assurer l’authenticité d’un message. L’empreinte du message est chiffrée à l’aide de la clé privée et est jointe au message. Les destinataires déchiffrent ensuite le cryptogramme à l’aide de la clé publique et retrouvent normalement l’empreinte. Cela leur assure que l’émetteur est bien l’auteur du message. On parle alors de signature ou encore de scellement.

**✠** La propriété des algorithmes asymétriques est qu’un message chiffré par une clé publique n’est lisible que par le propriétaire de la clé privée correspondante. À l’inverse, un message chiffré par une clé privée sera lisible par tous ceux qui possèdent la clé publique correspondante.

**✠** Ainsi avec sa clé privée, Anne :

🌢 Signe ses messages.

🌢 Lit (déchiffre) les messages qui lui sont adressés.

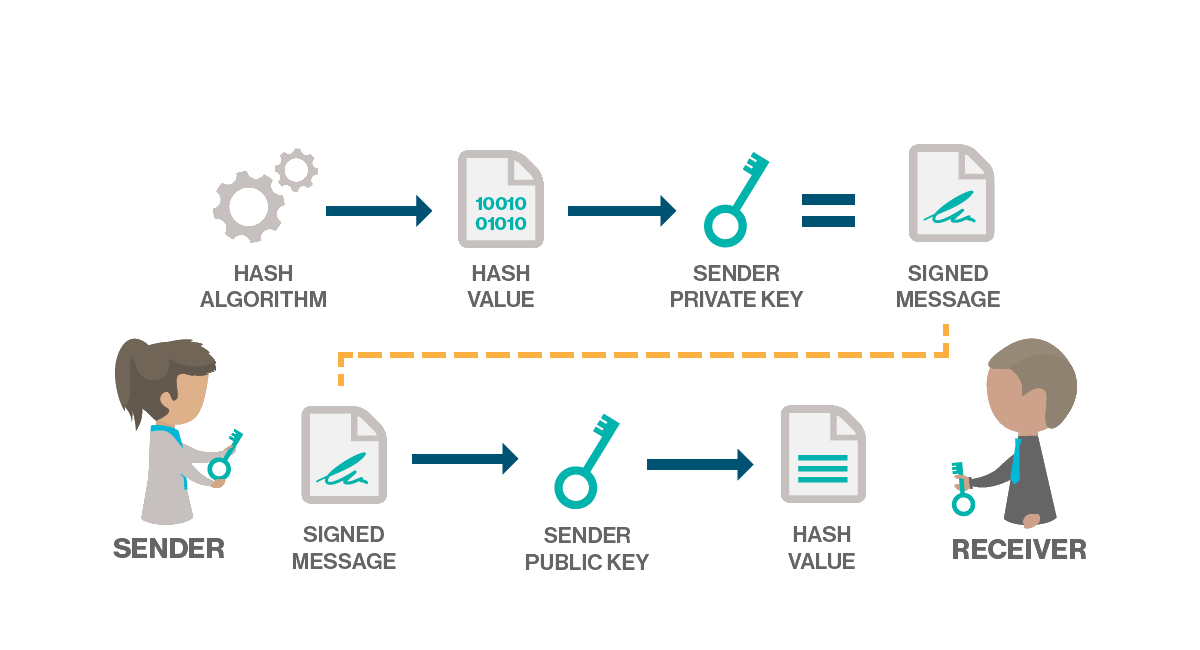
LES SIGNATURES DIGITALES :

**🕉** La signature digitale ou numérique - digital signature en anglais

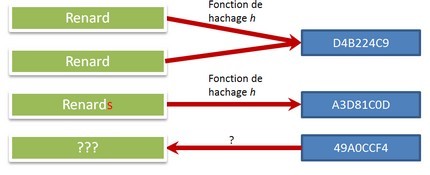
(À ne pas confondre avec un [certificat numérique](https://www.lemagit.fr/definition/Certificat-numerique)) est une technique de validation mathématique de l’authenticité et de l’intégrité d’un message, d’un logiciel ou d’un document électronique.

**🕉** Équivalent électronique, par essence plus sécurisé, d’une signature manuscrite ou de l’apposition d’un sceau, la signature numérique est une solution à la falsification et l’usurpation d’identité dans les communications électroniques. Elle constitue un élément supplémentaire prouvant l’origine, l’identité et l’état d’un document électronique, d’une transaction ou d’un message et démontre le consentement éclairé du signataire.

**🕉** Dans de nombreux pays, notamment aux États-Unis, les signatures digitales ont la même valeur juridique que les documents signés classiques. L’imprimerie nationale américaine « United States Gouvernement Printing Office » publie des éditions électroniques des lois de droit privé, public et du budget et des projets de loi du Congrès portant signature numérique.

**🌢** Fonction de la signature numérique **🌢**

LES FONCTION DE HASH :



**🕉** La Une fonction de hachage est une fonction qui convertit un grand ensemble en un plus petit ensemble, l’empreinte. Il est impossible de la déchiffrer pour revenir à l’ensemble d’origine, ce n’est donc pas une technique de chiffrement.

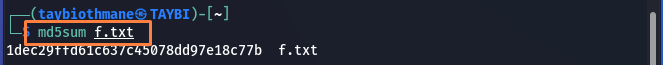
Quelques fonctions de hachage très utilisées :

🌢 MD5.

🌢 SHA-1.

🌢 SHA-256.

🌢 JH.



LES VPN :

**🕉** Un réseau virtuel privé, ou VPN, est un système qui réalise une connexion internet à l'aide d'un autre serveur. Il est situé, la plupart du temps, dans un autre pays, par le biais d'une connexion chiffrée. De cette manière, ce VPN vous fait bénéficier d'une adresse IP différente de celle qui vous est normalement attribuée. Vous pouvez ainsi cacher votre situation géographique réelle et surfer sur internet sous couvert d'anonymat.

Utilisé, à la base, principalement par des entreprises, de plus en plus de particuliers l'emploient aujourd'hui. Lorsque les employés voulaient accéder à l'intranet de leur entreprise à distance, et ce, de manière sécurisée, les VPN étaient un recours parfait.

