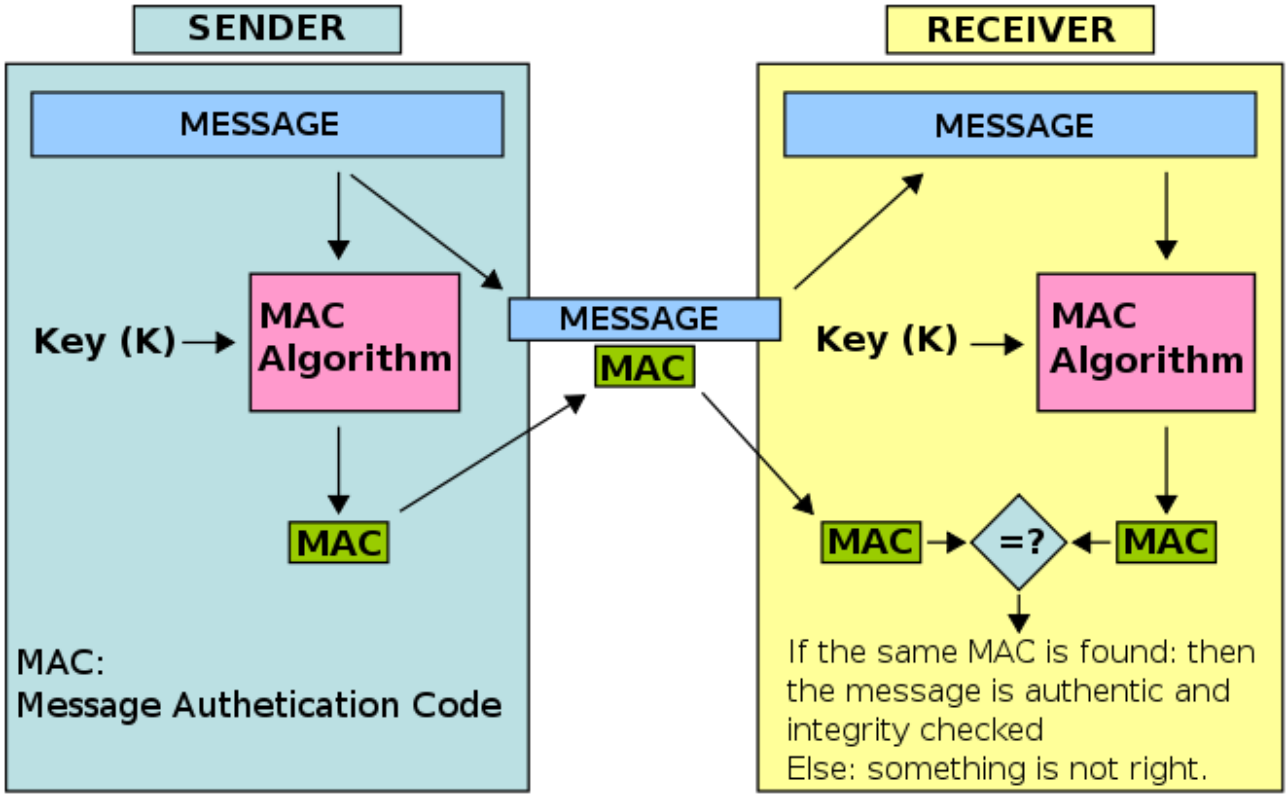
Projet TI : HMAC

réalisé par Nicolas FRANCOIS et Joseph LEFEVRE
projet encadré par Mme Rogozan

I) Introduction :

Un HMAC est un type de code d'authentification de message calculé au moyen d'une fonction de hachage et d'une clé secrète (H = Hash, MAC = Message authentification code). Ce type d'authentification continue à être utilisé aujourd'hui, notamment suite aux failles trouvées dans les fonctions de hachage cryptographique utilisées seules (failles du MD5, du SHA1, etc.).



Description du principe de l'HMAC

Ce document présentera le contenu du projet, la répartition des tâches, les outils utilisés, l'avancement actuel du projet et les problèmes rencontrés.

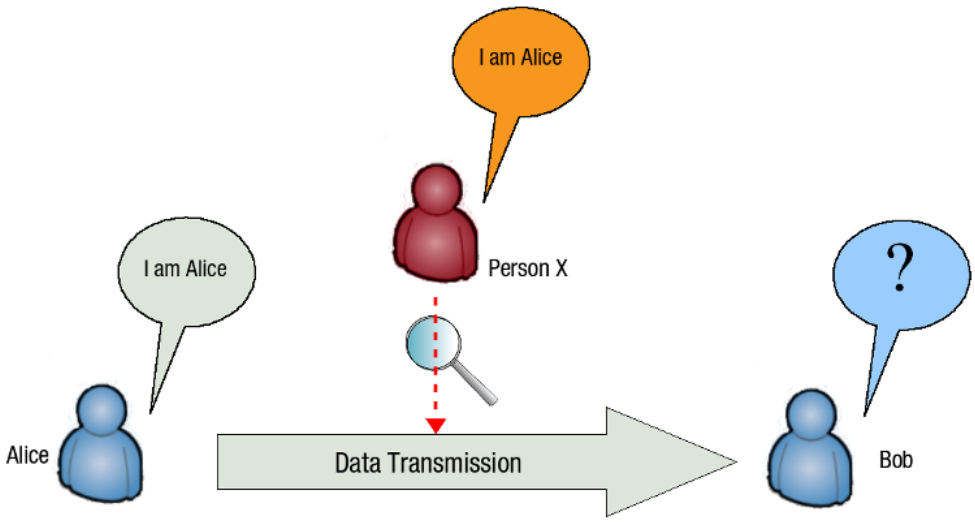
II) Contenu du projet :

Présentation du principe :

Durant ce projet, nous ferons un rappel sur les fonctions de hachage de la famille SHA et la fonction de hachage MD5. La raison de ce rappel est que ces fonctions sont au coeur des HMAC.
Nous ferons une présentation de l'histoire du HMAC, en expliquant le principe de ce dernier et en expliquant pourquoi ce type de code d'authentification est revenu ces dernières années au devant de la scène.

Sécurité :

Nous parlerons de son principal atout, qui est la résistance à la montée des ordinateurs quantiques, mais également quelques inconvénients. A travers cela nous ferons un bilan sur la sécurité du HMAC, en décrivant ses atouts et ses failles.



Utilisation :

Nous ferons aussi une interface graphique pour réaliser des calculs de signatures avec des HMAC (nous permettrons l'utilisation de différents algorithmes HMAC).

Applications :

Nous présenterons au moins une application concrète du HMAC, datant de ces dernières années.

III) Répartition des tâches :

Joseph s’occupera de décrire les applications du HMAC et utilisera des scripts pour effectuer des calculs de HMAC, tandis que Nicolas implémentera l’interface et fera appel aux fonctions manipulant le HMAC.
En ce qui concerne la présentation de l’HMAC, du SHA et du MD5, de même que la description de la sécurité de l’HMAC, ces tâches seront partagées entre les deux participants.

IV) Outils utilisés :

Pour réaliser ce projet, tout sera mis et archivé sur un dépôt Github (que ce soit le rapport, le code, les slides, etc.). Cela permettra au projet d’être accessible aux groupes qui ne pourront assister à la présentation.

Un outil qui sera probablement utilisé est la librairie OpenSSL. Cette librairie, très largement utilisés par le système d’exploitation Linux, implémente entre autre le HMAC. De nombreuses implémentations du HMAC se basent sur cette librairie (que ce soit en Python, en C, etc.) donc nous nous baserons également sur cette dernière pour réaliser nos scripts qui seront appelés par l’interface graphique.
En plus de l’utiliser, nous expliquerons son fonctionnement.

V) Références principales :

Pour ce projet, nous avons commencé à utiliser de nombreux documents. Voici la liste des documents ou sites sur lesquels nous nous sommes le plus appuyés jusqu’ici :
- Un article de Cisco dont la dernière mise à jour date d’octobre 2015 (http://www.cisco.com/c/en/us/about/security-center/next-generation-cryptography.html#4)

- Un cours sur l'authentification de messages créé par un enseignant à l'IRISA (https://www.irisa.fr/prive/sgambs/cours4_intro_securite.pdf)
- Un article du NIST (national institute of standard and technology) sur le HMAC posté en 2008 (http://csrc.nist.gov/publications/fips/fips198-1/FIPS-198-1_final.pdf)
- Les articles Wikipédia en anglais sur le HMAC, le SHA et le MD5.

VI) Avancement du projet

Nous avons défini les algorithmes à utiliser, et avons posé les bases de l'implémentation de ces derniers. Il ne reste plus qu'à faire l'interface graphique et à rendre le script plus générique (étant donné que tout est sur Github nous allons faire du code le plus propre possible).
Nous avons pour le moment surtout fait un travail de documentation, et avons préparé un premier exemple concret d'applications. Il nous reste tout le diaporama à faire.
Il nous reste également l'étude des failles de sécurité du HMAC à approfondir et à expliquer.