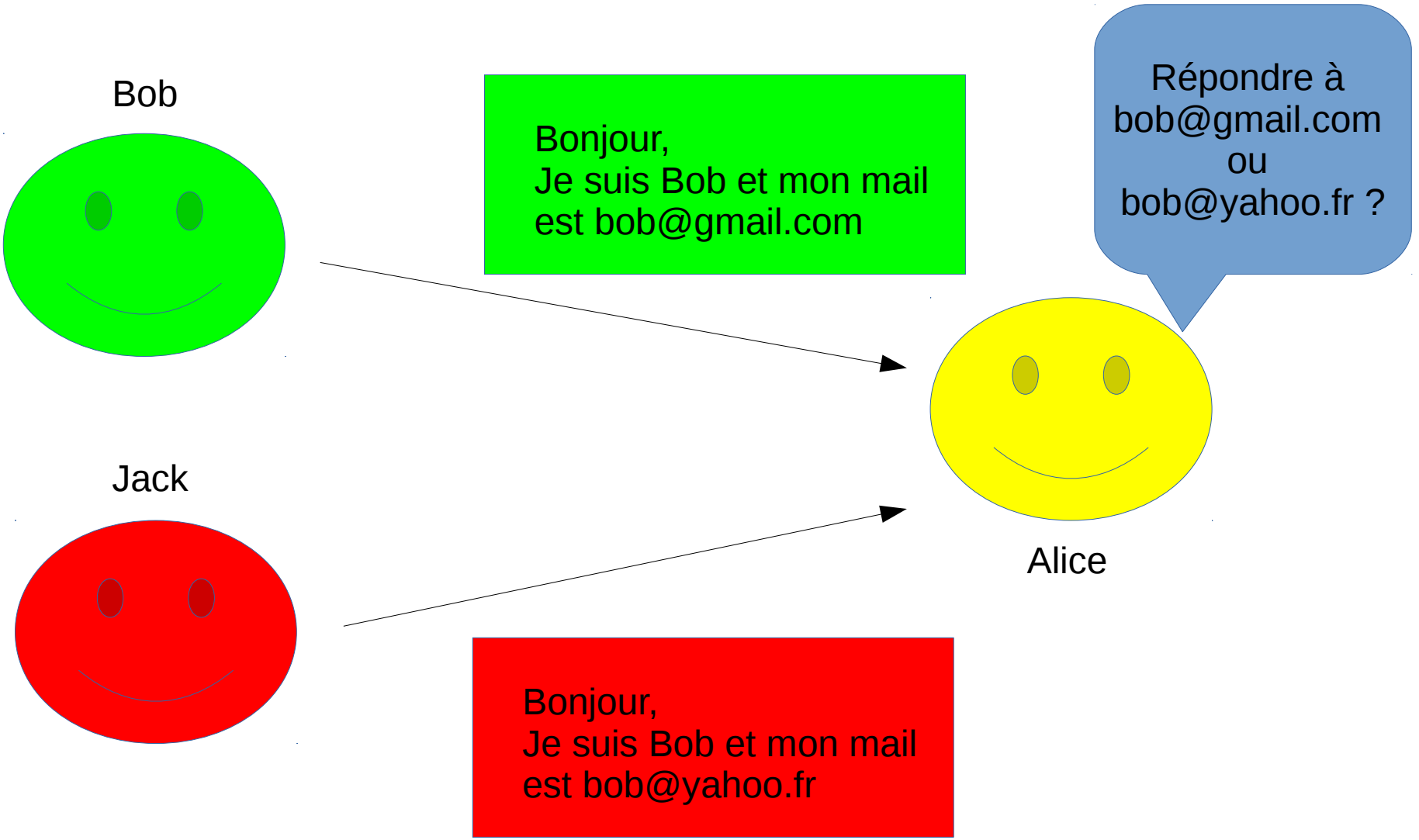
HMAC

Hashed Messeage authentification code

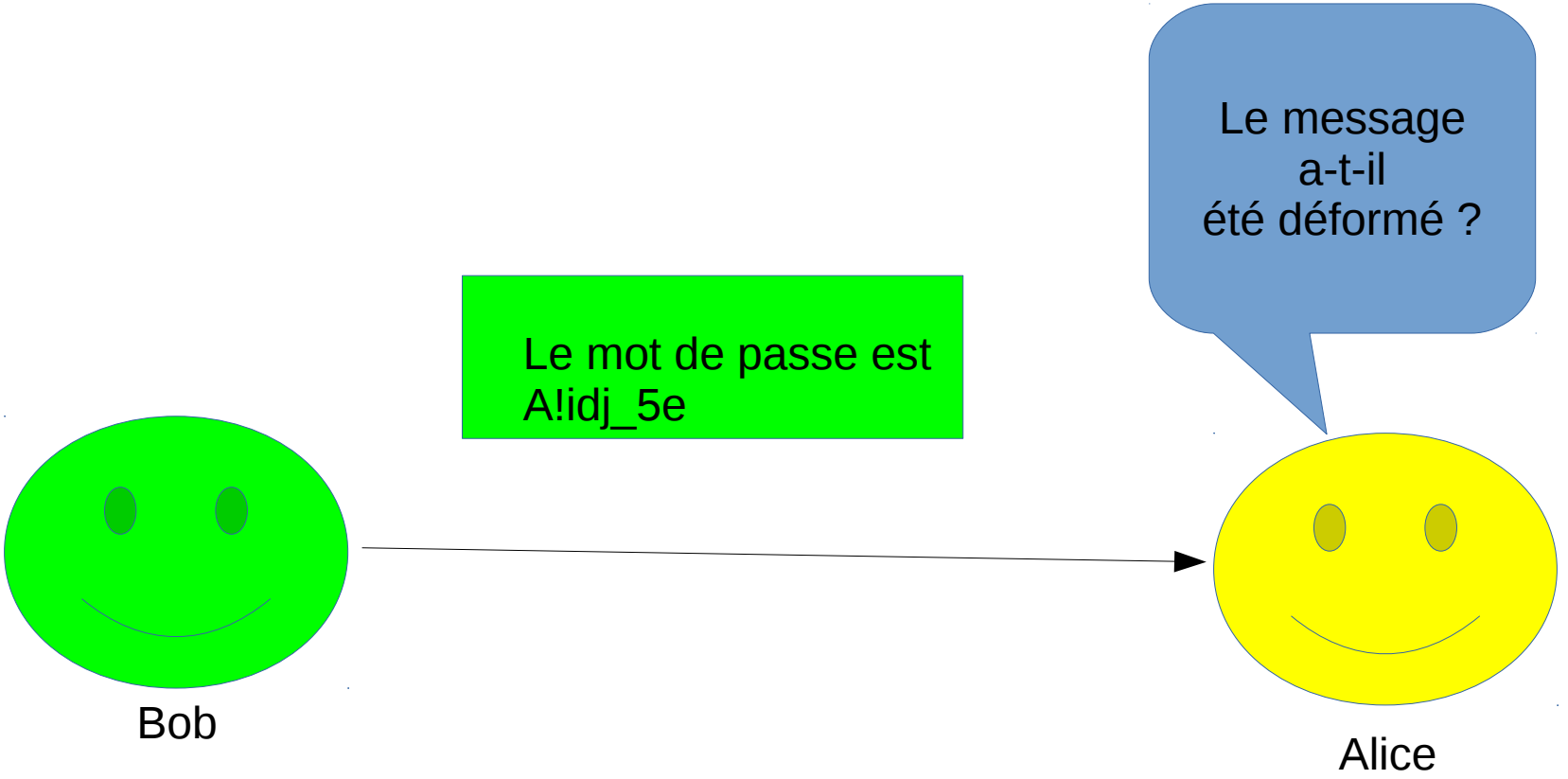
par Nicolas FRANCOIS et Joseph LEFEVRE

décembre 2016

Authentification

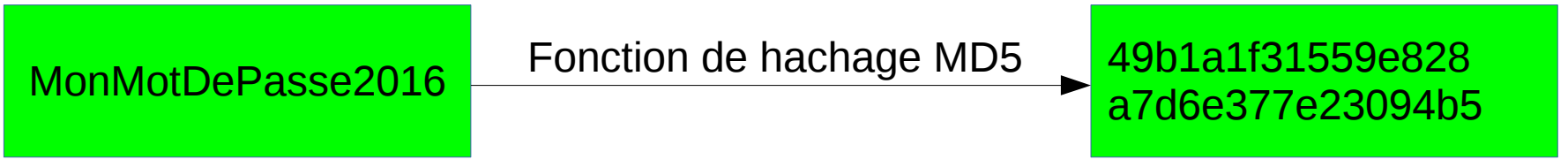


Intégrité

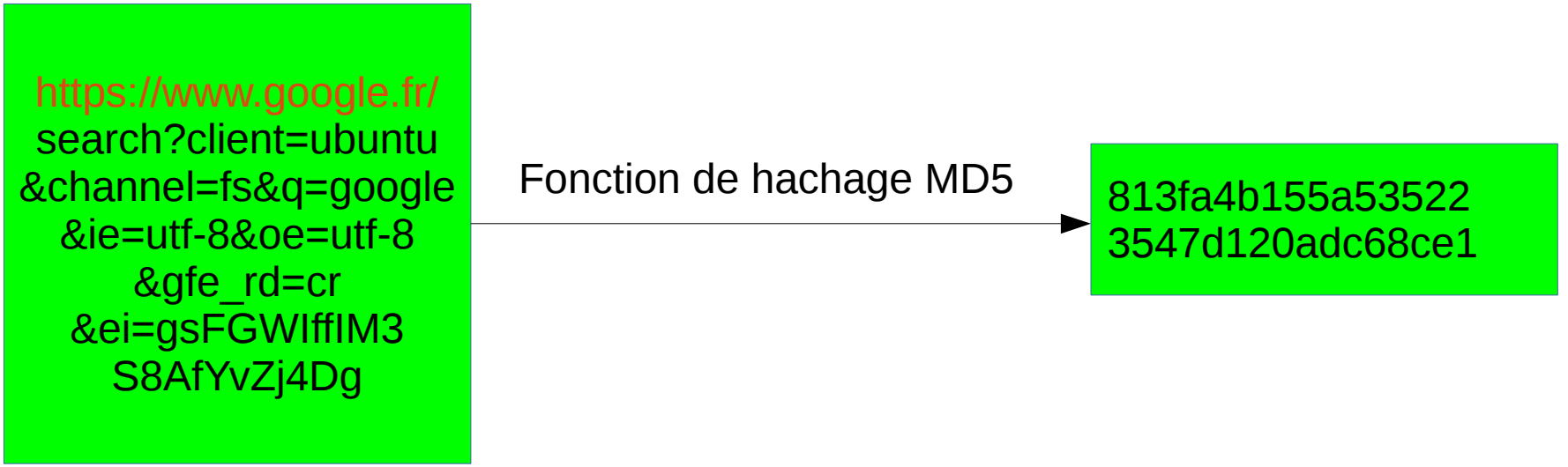

Le message
a-t-il
été déformé ?
Le mot de passe est
A!idj_5e
Bob
Alice

Fonction de hachage

Vérifier le mot de passe



Vérifier l'intégrité d'un texte



Fonction de hachage : Collision

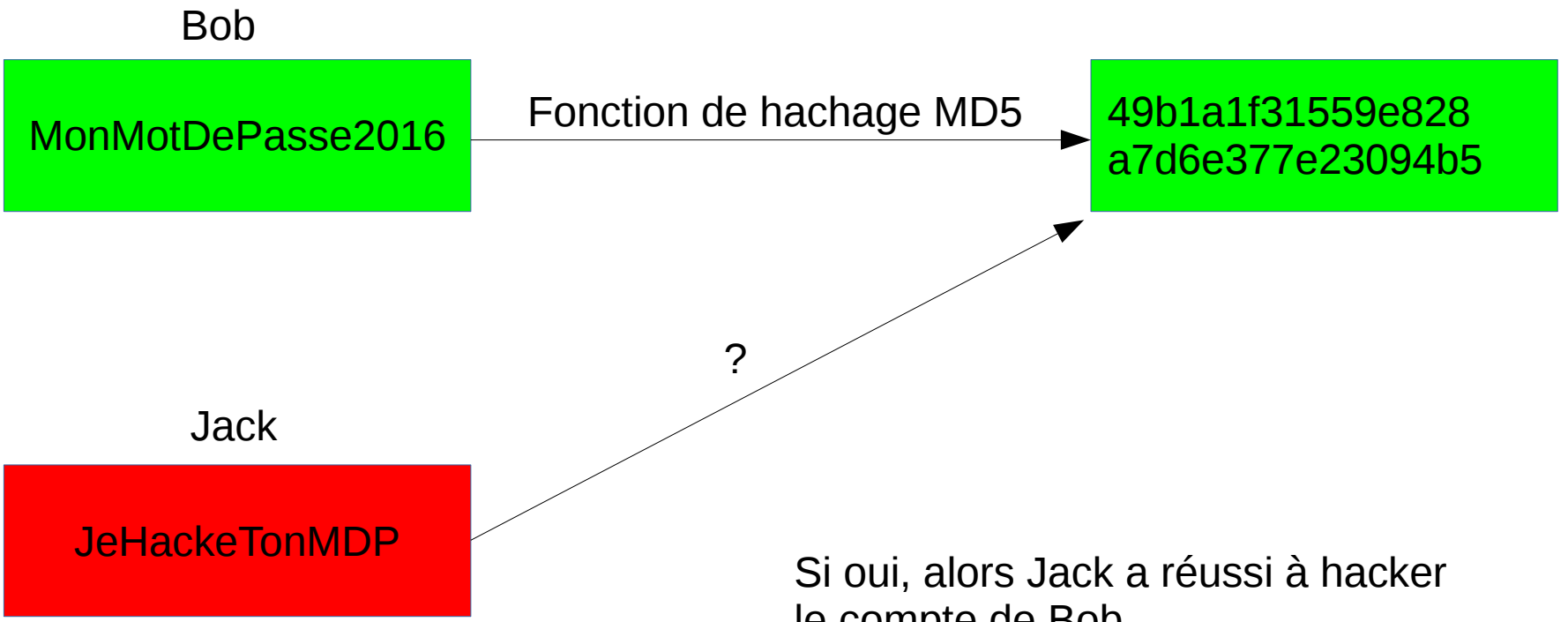
MD5

MD5

253dd04e87492e4
fc3471de5e776bc3d

Images de http://natmchugh.blogspot.fr/2015/02/create-your-own-md5-collisions.html

Fonction de hachage : Risque



Retour sur le HMAC

Principe d'un MAC

(MAC : message authentification code)

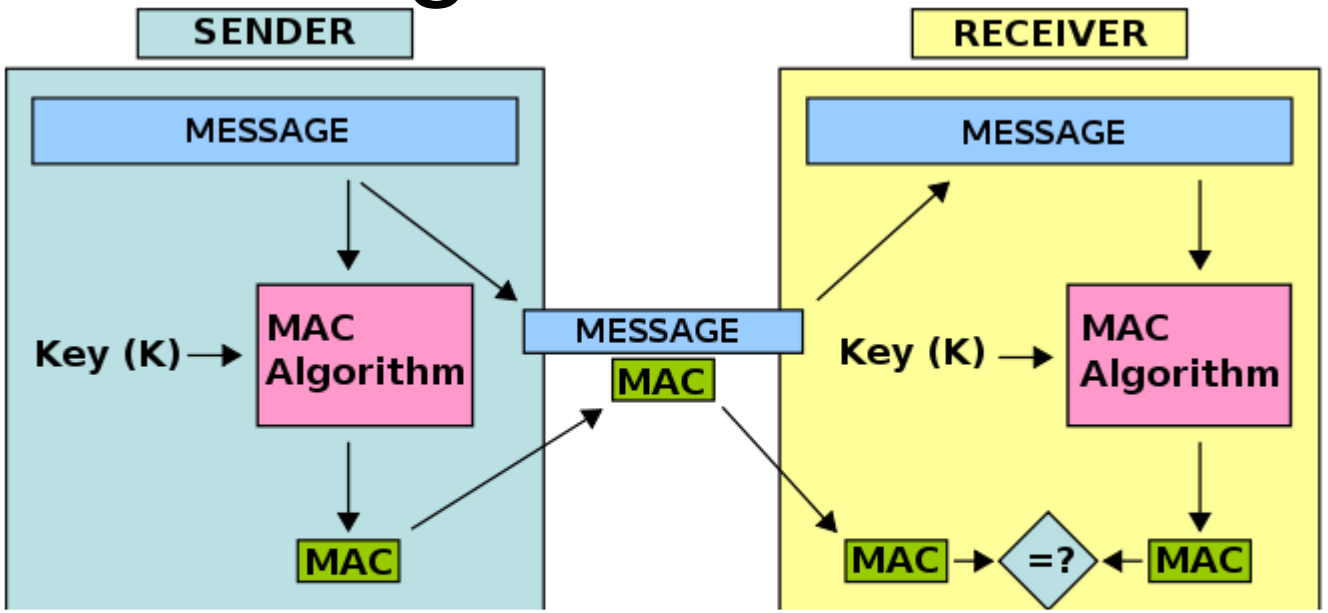


Image de http://stackoverflow.com/questions/9922085/clarification-on-hmac-authentication-with-wcf

La formule du HMAC :

HMAC(K,M) =H[(K+ XOR opad) || H[(K+ XOR ipad) || M]].

H = fct hachage
M = message
L = number of blocks in
B = nb de bits d'un bloc
K = clé secrète
K+ = K avec des zéros à gauche
(pour attendre taille de b bits)
Ipad = 36 (en hexa) répété b/8 fois
Opad = 5C (en hexa) répété b/8 fois

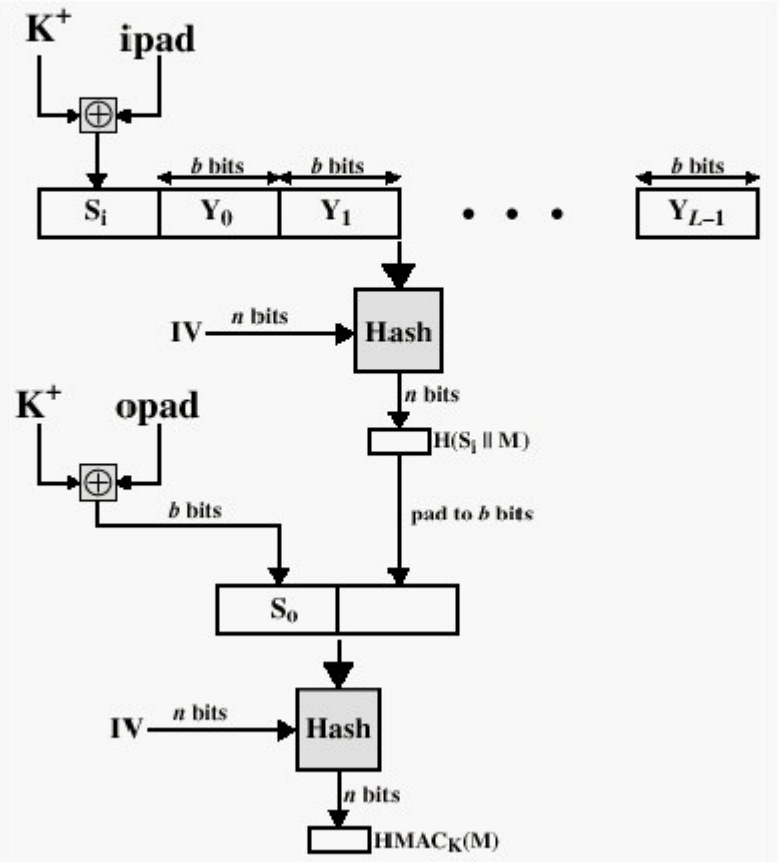


Image de http://www.slideshare.net/koolkampus/chapter-ns3

Démonstration !

Application 1 : Mysensors

Image de https://www.mysensors.org/

Application 2 : AngularJS

Intérêt : Eviter le «Man in the middle»

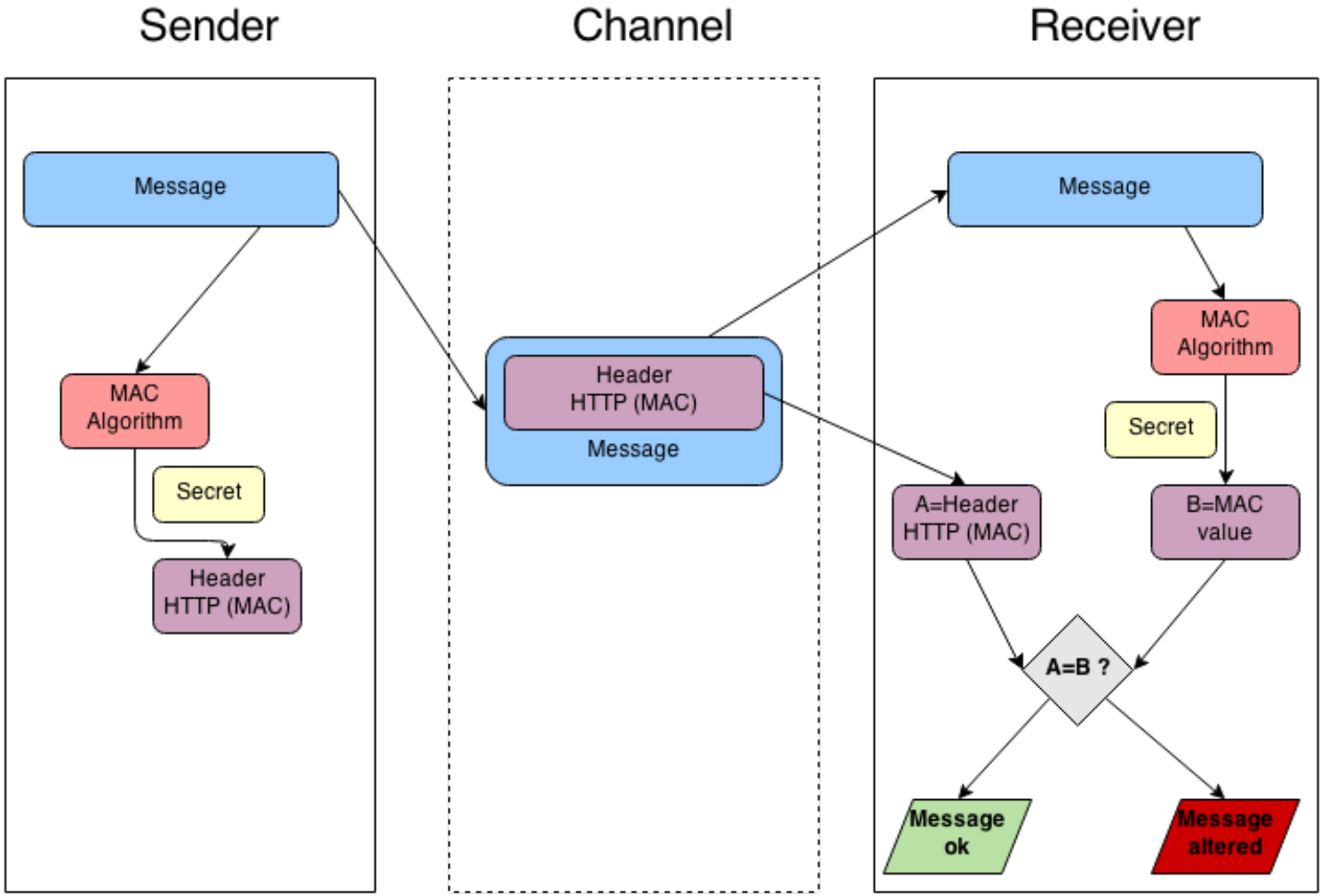


Image de https://www.redfroggy.fr/securisez-vos-applications-angular-avec-spring-security-et-hmac/