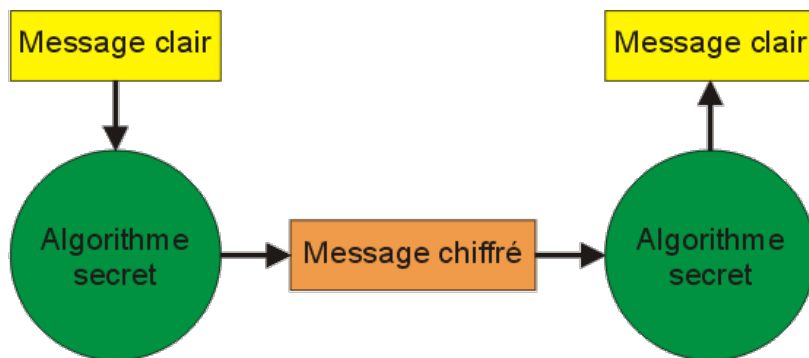


I - Introduction

La **cryptographie** consiste à chiffrer des données pour les rendre **confidentielles**. C'est la base de tout échange d'informations **sécurisé**.

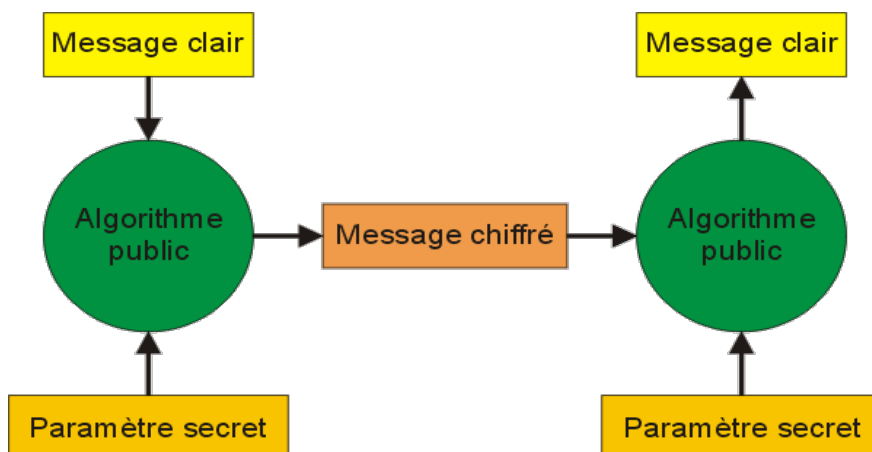
II - Sécurisation d'un dialogue avec un algorithme secret

Ici on dispose d'un **algorithme de chiffrement secret** qui assure à lui seul la confidentialité du message. Un tel procédé, cependant, n'est pas considéré comme sûr, si quelqu'un réussit à reconstituer l'algorithme alors il n'y aura plus de secret.



III - Sécurisation d'un dialogue avec un algorithme et une clé

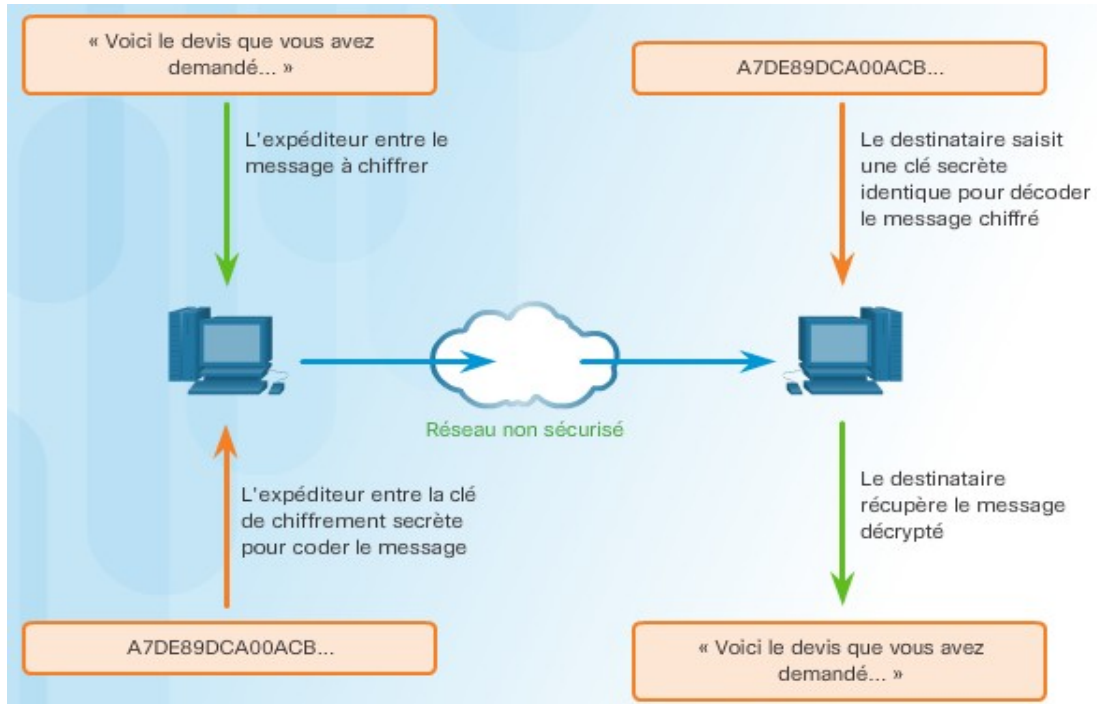
Ici on utilise un **algorithme de chiffement public**, que tout le monde peut analyser et utiliser, mais qui exploitera un paramètre de chiffement (**clé de chiffement**) qui, lui ne sera pas partagé.



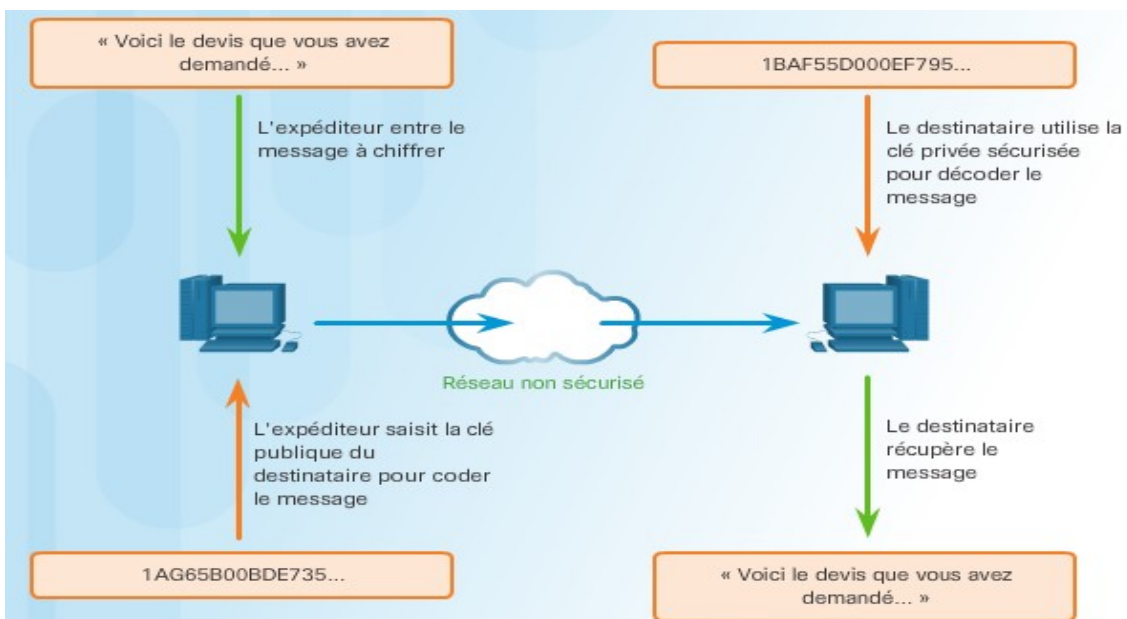
Ce principe, qui peut éventuellement adopter des **combinaisons de clés**, reste à l'heure actuelle le procédé le plus sûr. Ici, pour déchiffrer le message, il faudra la bonne clé, l'algorithme étant public.

IV - Chiffrement Symétrique et Asymétrique

Chiffrement Symétrique : On utilise **une clé** de chiffrement et de déchiffrement identiques.
Inconvénient : Comment transmettre cette clé de chiffrement en toute sécurité ?



Chiffrement Asymétrique : On utilise 2 clés, une **clé publique** qui peut être partagée et une **clé privée**.
Ce qui est **chiffré** avec une **clé publique** ne peut être **déchiffré** qu'avec la **clé privée correspondante**.

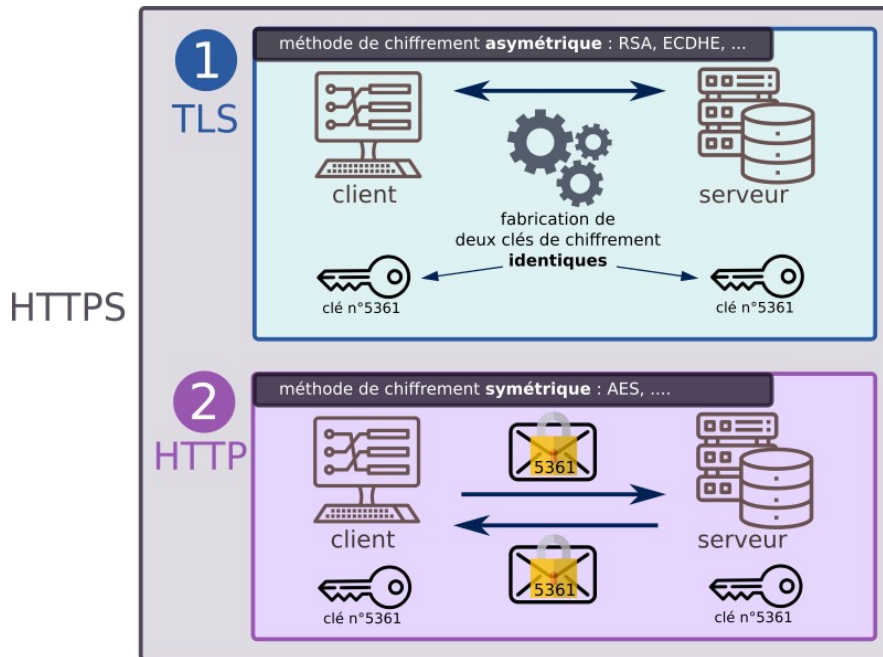


Remarque : La **clé publique** est unique, il suffit de la récupérer via un **certificat numérique signé** par un dépositaire, dit « **tiers de confiance** » ou **CA** : Certificate Authority.

V - Le protocole HTTPS

Le protocole **HTTPS** est la réunion de deux protocoles :

- le protocole **TLS** (Transport Layer Security, qui a succédé au **SSL**) : ce protocole, basé sur du **chiffrement asymétrique**, va conduire à la génération d'une clé identique chez le client et chez le serveur.
- le protocole **HTTP**, mais qui convoiera maintenant des données chiffrées avec la clé générée à l'étape précédente. Les données peuvent toujours être interceptées, mais sont illisibles. Le **chiffrement symétrique** utilisé est actuellement le chiffrement **AES-128** ou **AES-256**.



Lors de l'ouverture d'une communication **HTTPS**, le serveur envoie son **certificat** contenant la **clé publique**. Soit ce certificat est dans une liste de certificats provenant d'un **organisme de confiance (CA : Autorité de certification)** soit il est dit « **auto-signé** » et le client peut l'accepter à ses risques et périls.

Lorsqu'on s'adresse à un **organisme de confiance (CA)** pour récupérer une **clé publique**, il l'envoie avec un **certificat numérique signé**. Les certificats sont à la norme **X.509**.

Par exemple un navigateur installe des certificats de divers organismes qui contiennent une clé publique :

