

Introduction à la Cryptographie





Mise au point sur les définitions

Chiffrement asymétrique

- C
-
-
- C
- déc
- E
- H

Chiffrement	Déchiffrement
<p>Message Clé Publique Alice</p> <p>Message chiffré</p>	<p>Message chiffré Clé Privée Alice</p> <p>Message</p>



Autres concepts

- ◉ **L'histoire de Bob et Alice**
- ◉ **Tiers de confiance**
- ◉ **Infrastructure à clés publiques**



Bob & Alice

- ◉ Alice communique avec **Bob**
- ◉ Utilisation d'une histoire avec des personnages pour simplifier les explications
- ◉ Autres caractères : **Eve & Mallory**



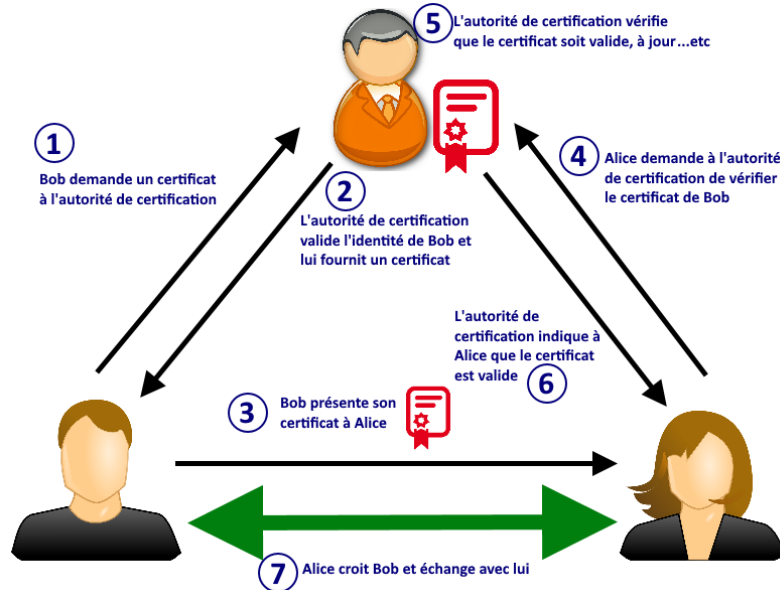
Tiers de confiance

- ◉ **Nécessaire pour l'échange de clés** (chiffrement à clé publique)
- ◉ Comment croire les entités avec lesquelles on communique ?
- ◉ Nécessité d'un tiers de confiance (*Verisign, DigiCert...etc*)
- ◉ Services de certification considérés comme **étant de confiance**
- ◉ Utilisation de **certificat**



Infrastructure à clés publiques

- Infrastructure permettant de **créer, gérer, délivrer, révoquer des certificats**





Création d'un certificat

