3TI

Sécurité des réseaux informatiques

2015-2016

Bases de cryptographie

V.Van den Schrieck

Prélude

Aimons et admirons le chancelier Hitler
L'éternelle Angleterre est indigne de vivre
Maudissons, écrasons le peuple d'outre-mer
Le Nazi sur la terre sera seul à survivre
Soyons donc le soutien du Führer allemand
De ces navigateurs la race soit maudite
A eux seuls appartient ce juste châtiment
La palme du vainqueur répond au vrai mérite

Brainstorming

- C'est quoi, la crypto?

Prélude

Petit exercice de cryptanalyse

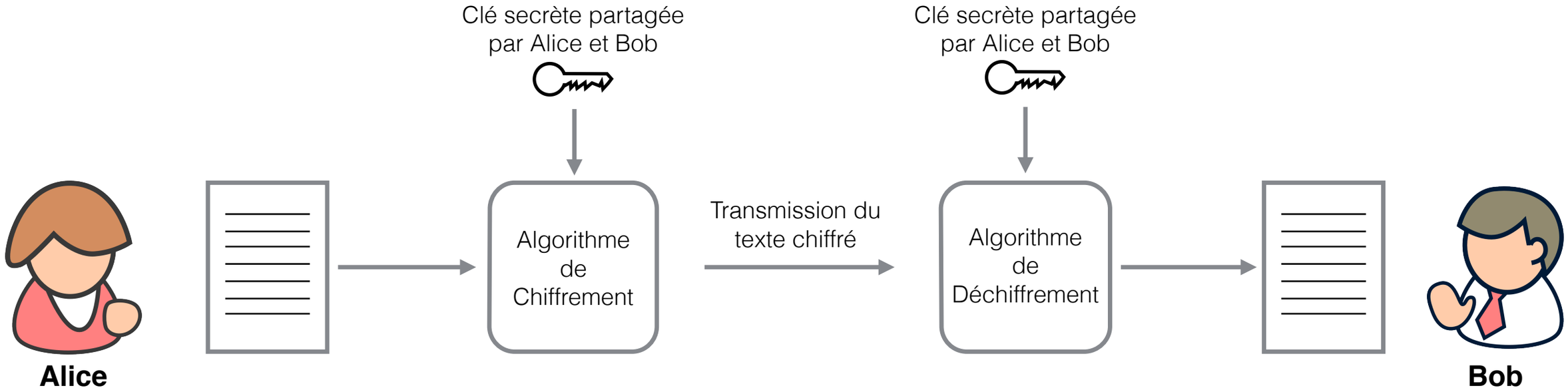
Prélude

Sur base de ce que vous avez fait au TP, énoncez des conditions sur le chiffrement pour garantir la confidentialité d'une communication

Indice : Différence entre exercice sur papier et craquage du code de César?

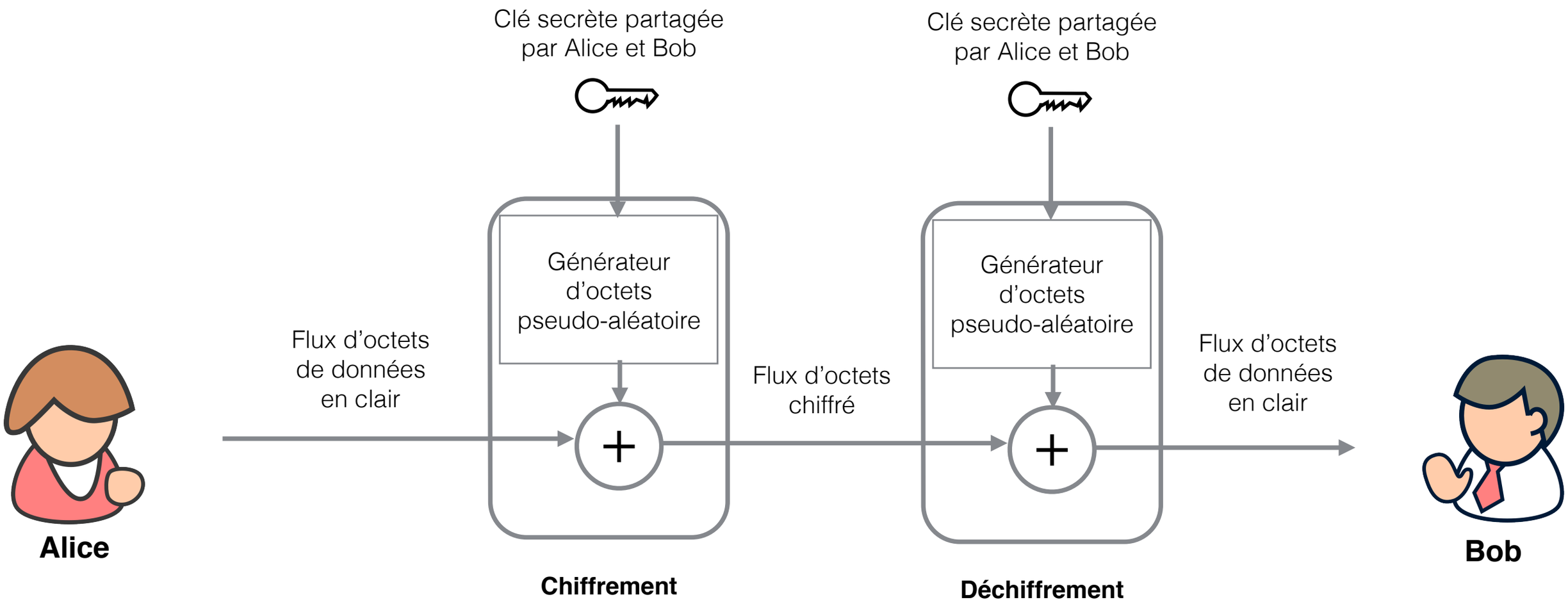
Par groupes de 3 - 10 minutes

Confidentialité



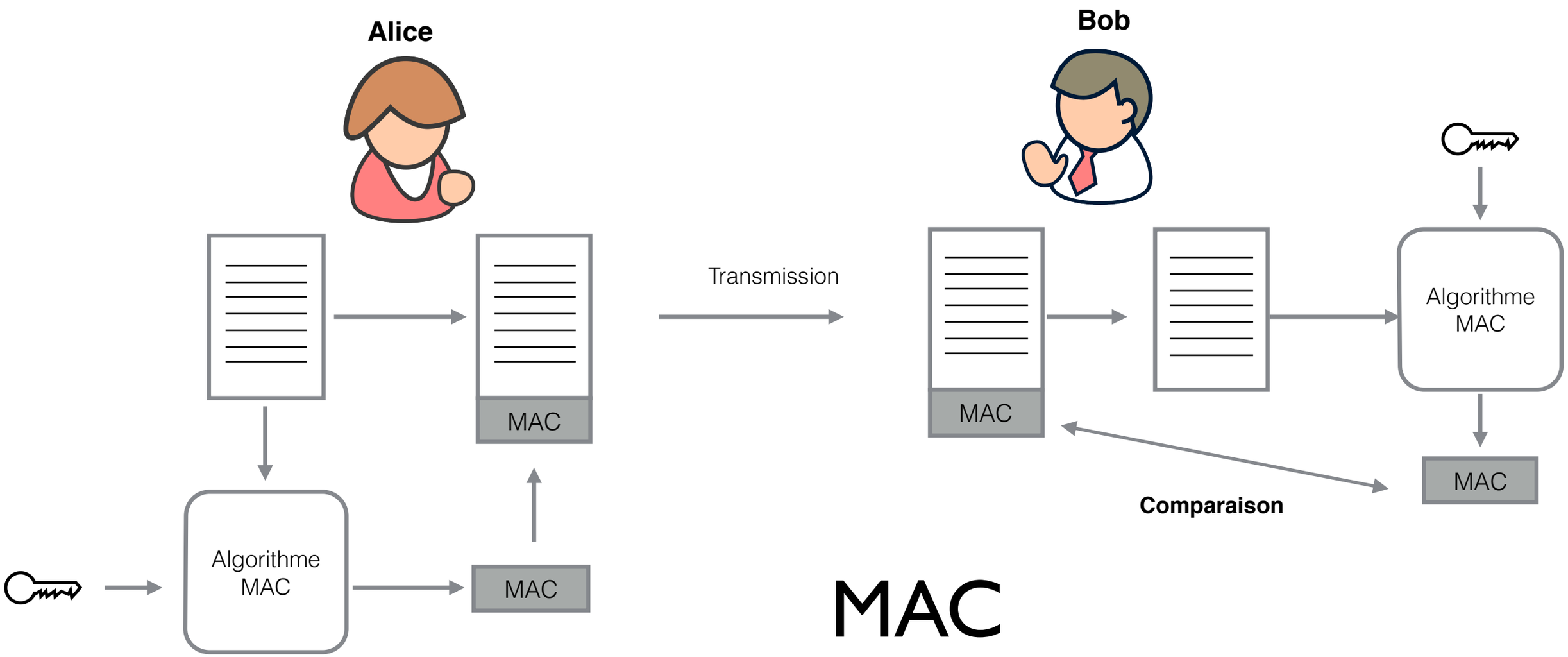
Chiffrement symétrique

Confidentialité



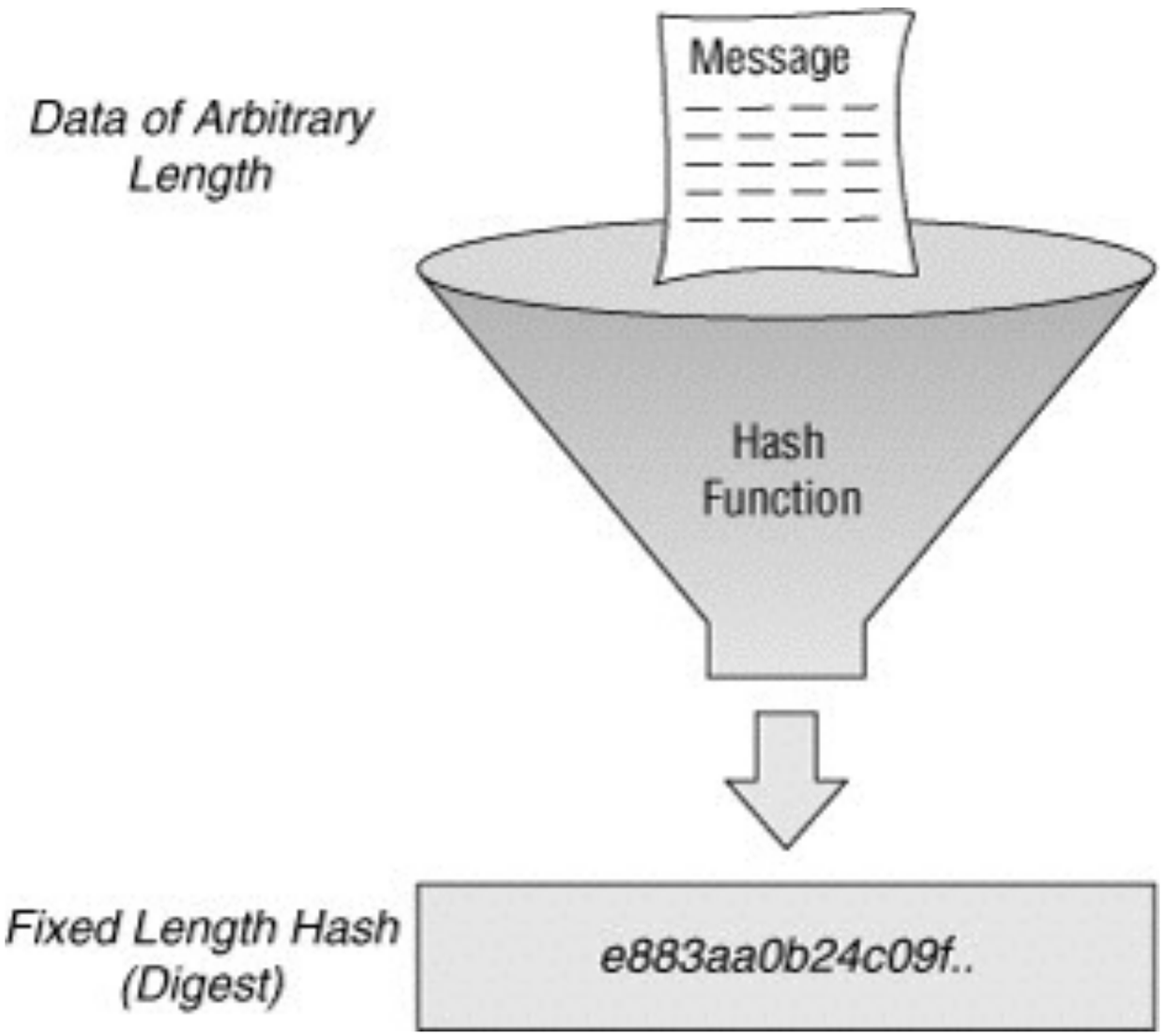
Chiffrement symétrique par flux

Authentification de messages

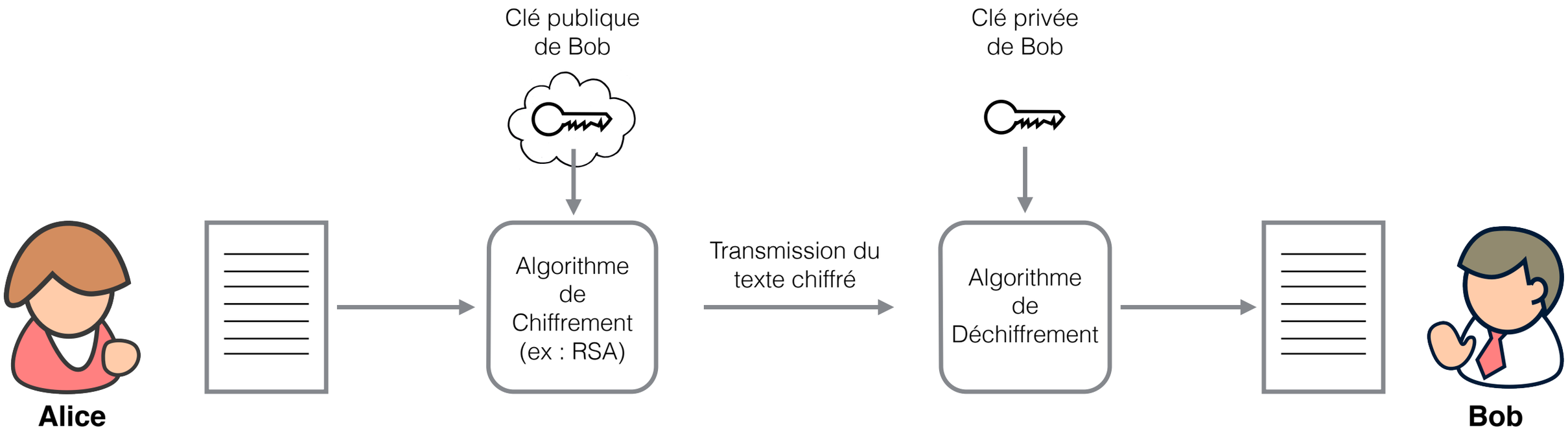


MAC

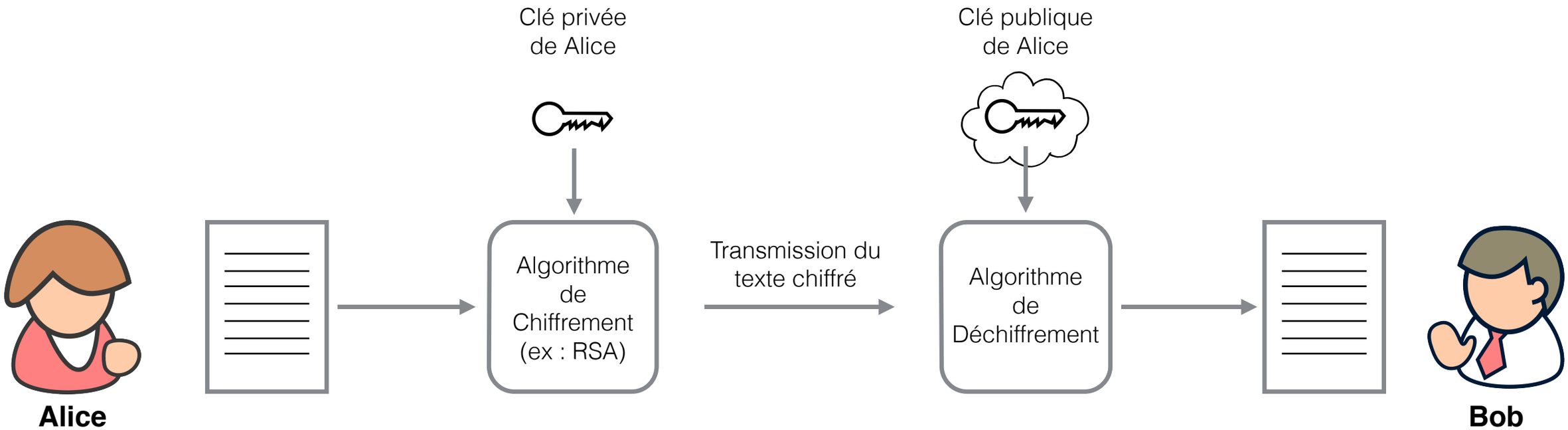
Fonctions de hachage



Cryptographie asymétrique



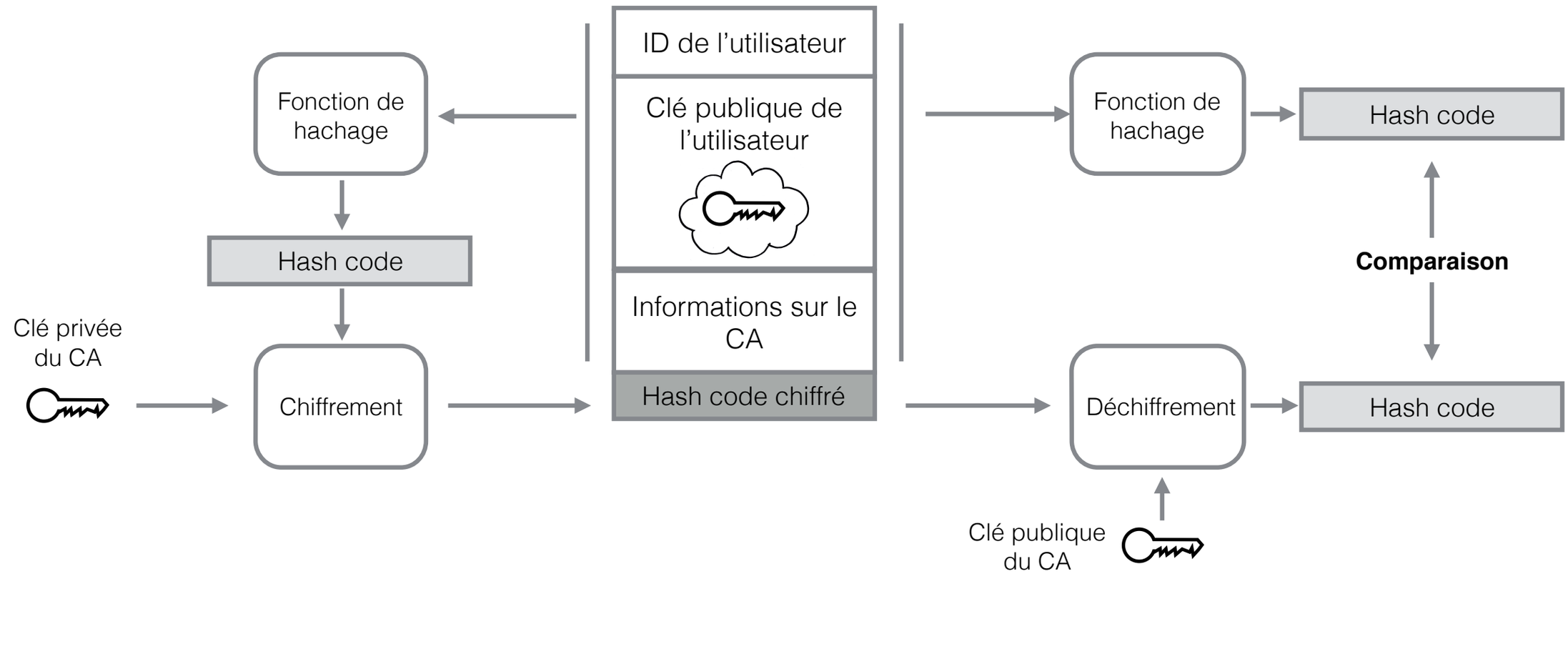
Cryptographie asymétrique



Utilisation de la crypto asymétrique

- Signature numérique
- Gestion des clés
  - Certificat de clé publique
  - Distribution de clé secrètes
  - Enveloppes numériques

Certificat de clé publique



Algorithmes de crypto asymétrique

Algo	Signature numérique	Partage de clé symétrique	Chiffrement de clé secrète
RSA	Oui	Oui	Oui
Diffie Hellman	Non	Oui	Non
DSS	Oui	Non	Non
ECC	Oui	Oui	Oui

Discussion

Par groupe de 3 : Quand utilisez-vous la cryptographie asymétrique dans votre vie quotidienne? Et la cryptographie symétrique?