Réseaux et sécurité

F. Brunet – 12 novembre 2009

Plan

- Généralités
- Éléments techniques
  - Cryptographie symétrique
  - Cryptographie asymétrique
  - Authentification

Enjeux et risques

- La TM repose lourdement sur les réseaux
- La confidentialité des données doit être assurée
- L’identité réelles des utilisateurs doit aussi être assurée

Domaines

- Éléments « avancés » de TM : téléconsultation, télé-expertise, télé staff, etc.
- Mais aussi :
  - Intranet (« hôpital ville »)
  - Messagerie
  - Transmission des feuilles de soins (carte vitale)
  - Bref, dès lors que de l'information sensible transite, il faut que ce soit de manière sécurisée

Exemple : le RSS

- RSS = Réseau Santé Social
- Réseau utilisé par le système SESAM-VITALE
  - Dossier pharmaceutique
  - Carte vitale
- Initialement (1997) : réseau dédié
  - Opéré par Cegetel
- Aujourd'hui : couche de service et de sécurité sur des connexions internet classique
  - Fournisseur d'accès du RSS : SFR

Cryptographie symétrique

- La clé (ou la méthode de chiffrement) doivent être connu à la fois de l'émetteur et du récepteur

- Exemples
  - Substitutions
  - Enigma
  - Dictionnaire

Cryptographie symétrique

- Défaut : émetteur et récepteur doivent partager la clé

- Avantage : méthodes rapides

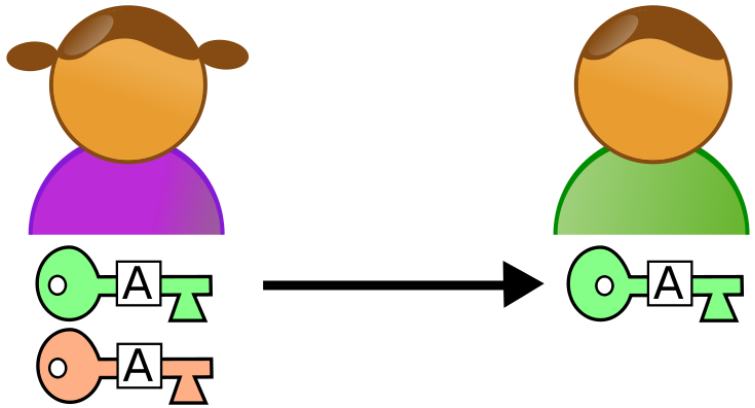
Cryptographie asymétrique

- Cryptographie asymétrique ou cryptographie à clé publique
- Logiciels : PGP, GnuPG, OpenSSL

- Repose sur des *fonctions à sens unique et à brèche secrète*
  - Fonction difficile à inverser à moins de connaître la brèche secrète : la clé privée

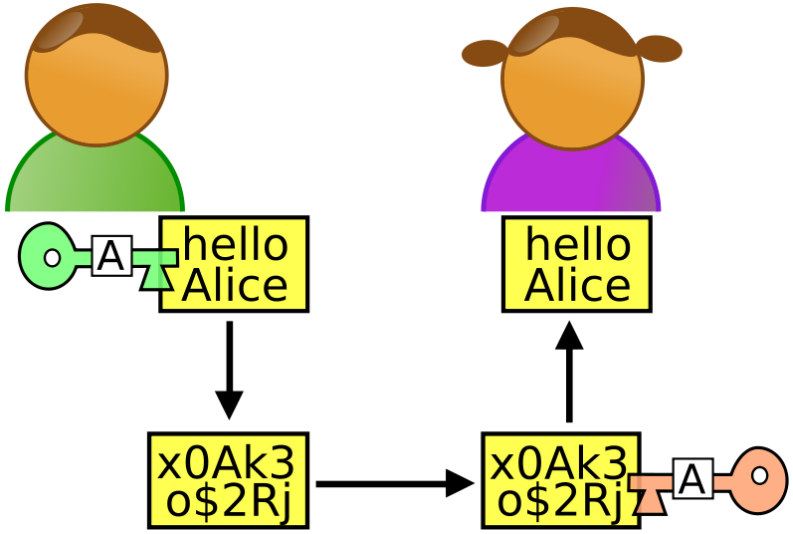
Cryptographie asymétrique

- Alice veut pouvoir recevoir des messages chiffrés de n'importe qui
- Alice génère 2 clés
  - La clé publique (verte) qu'elle diffuse à tout le monde
  - La clé privée (rouge) qu'elle conserve sans la divulguer



Cryptographie asymétrique

- Bob chiffre le message avec la clé publique d'Alice et envoie le texte chiffré
- Alice déchiffre le message avec sa clé privée



Cryptographie asymétrique

- $N = p\ q$ avec p et q des nombres premiers
- Calculer N à partir de p et de q est très facile
- L'inverse, c'est-à-dire trouver p et q tels que $N = p\ q$ est beaucoup plus difficile

- Du coup :
  - Clé publique à base de N
  - Clé privée à base de p et de q

Cryptographie asymétrique

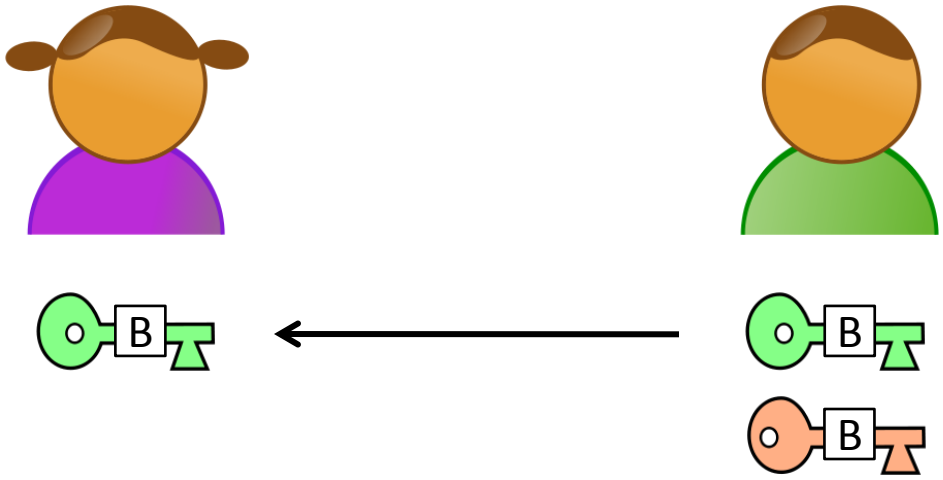
- Avantage : pas besoin d'échanger la clé secrète
- Inconvénient : processus de chiffrement généralement long
- Combinaison symétrique/asymétrique

Authentification

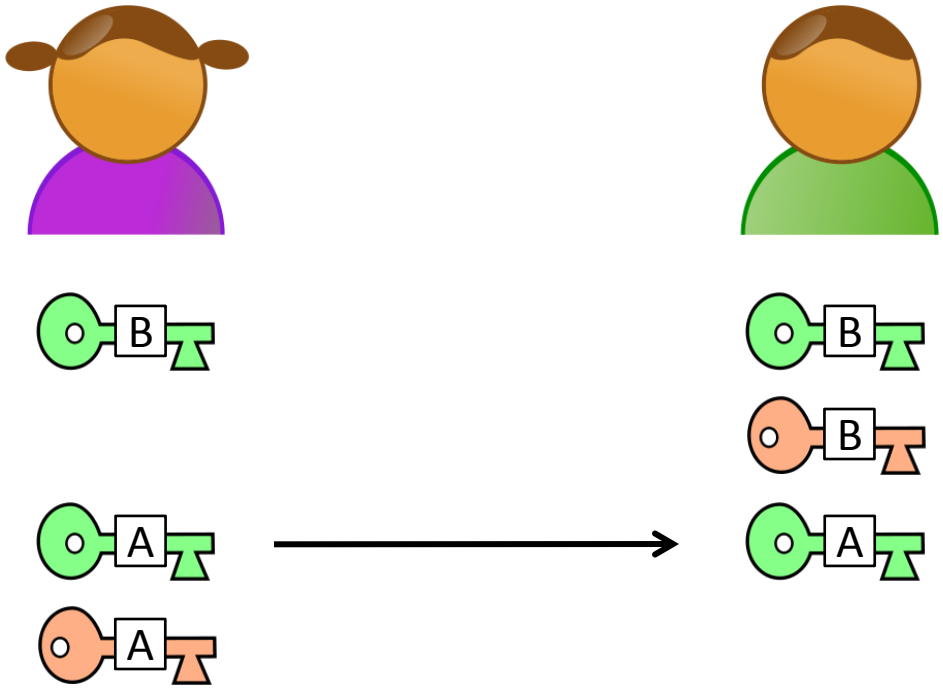
- Chiffrer les messages est insuffisant pour garantir la confidentialité des données médicales (ou autre)

- Le destinataire doit aussi s'assurer de qui provient un message : athentification

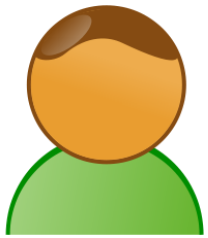
1) Bob crée une paire de clés asymétriques : il conserve la clé privée et diffuse librement la clé publique (notamment à Alice).

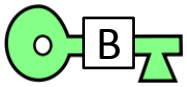


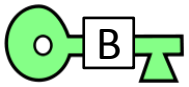
2) Alice crée une paire de clés asymétriques : clé privée (qu'elle conserve), clé publique (qu'elle diffuse librement, notamment à Bob).

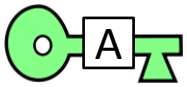


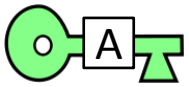
3) Bob effectue un *condensat* de son message « en clair » puis chiffre ce condensat avec *sa propre clé privée*.

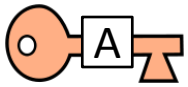


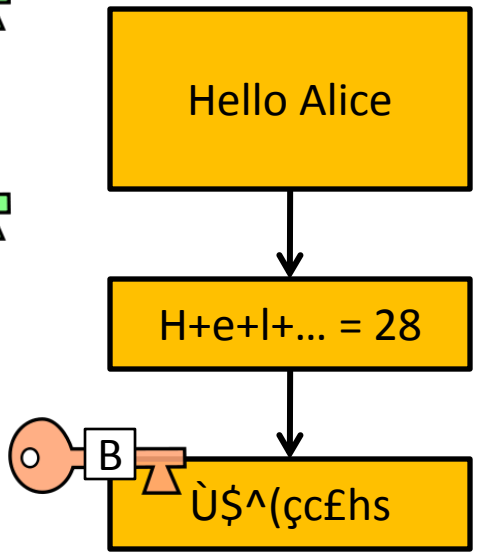




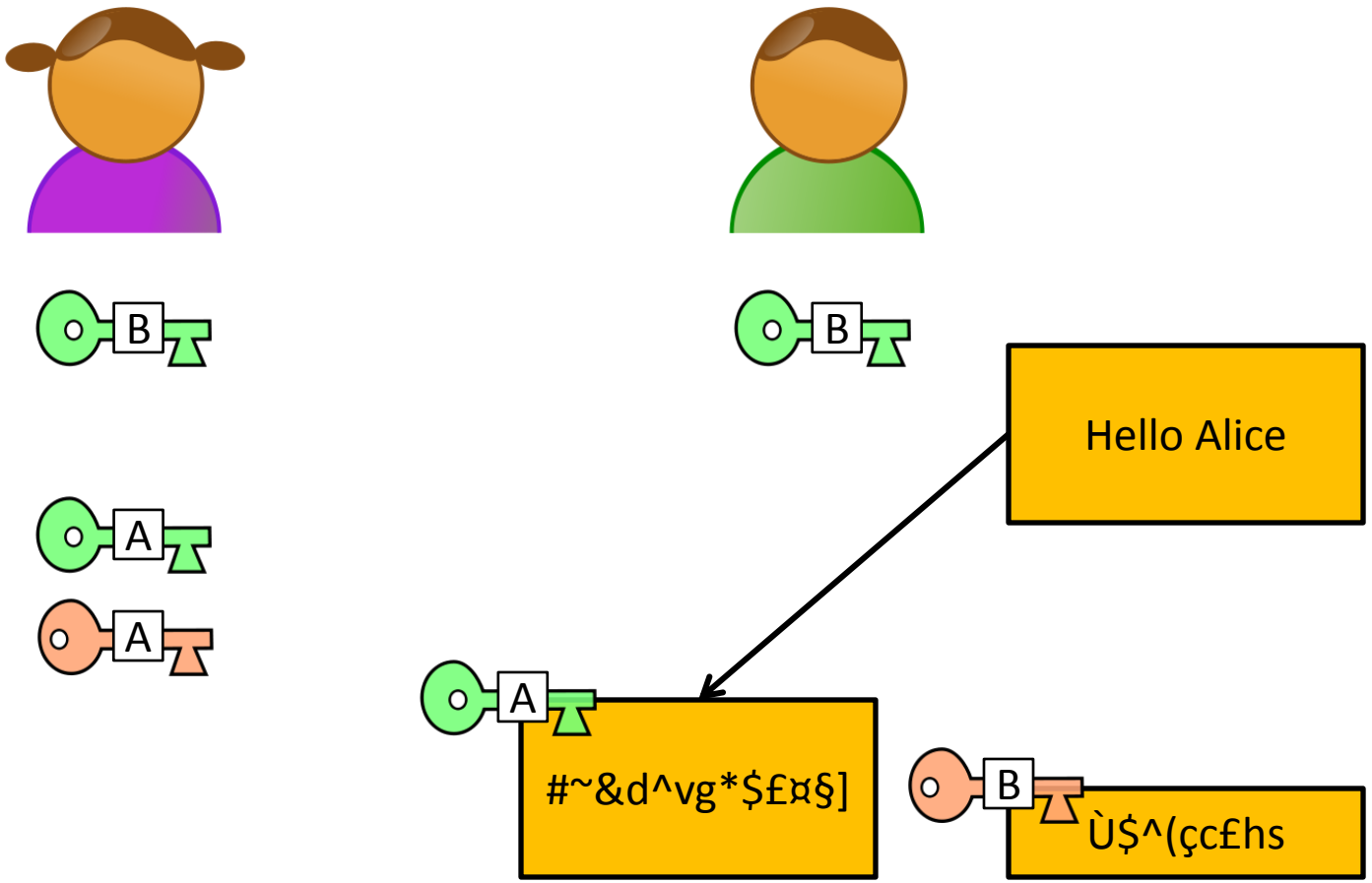




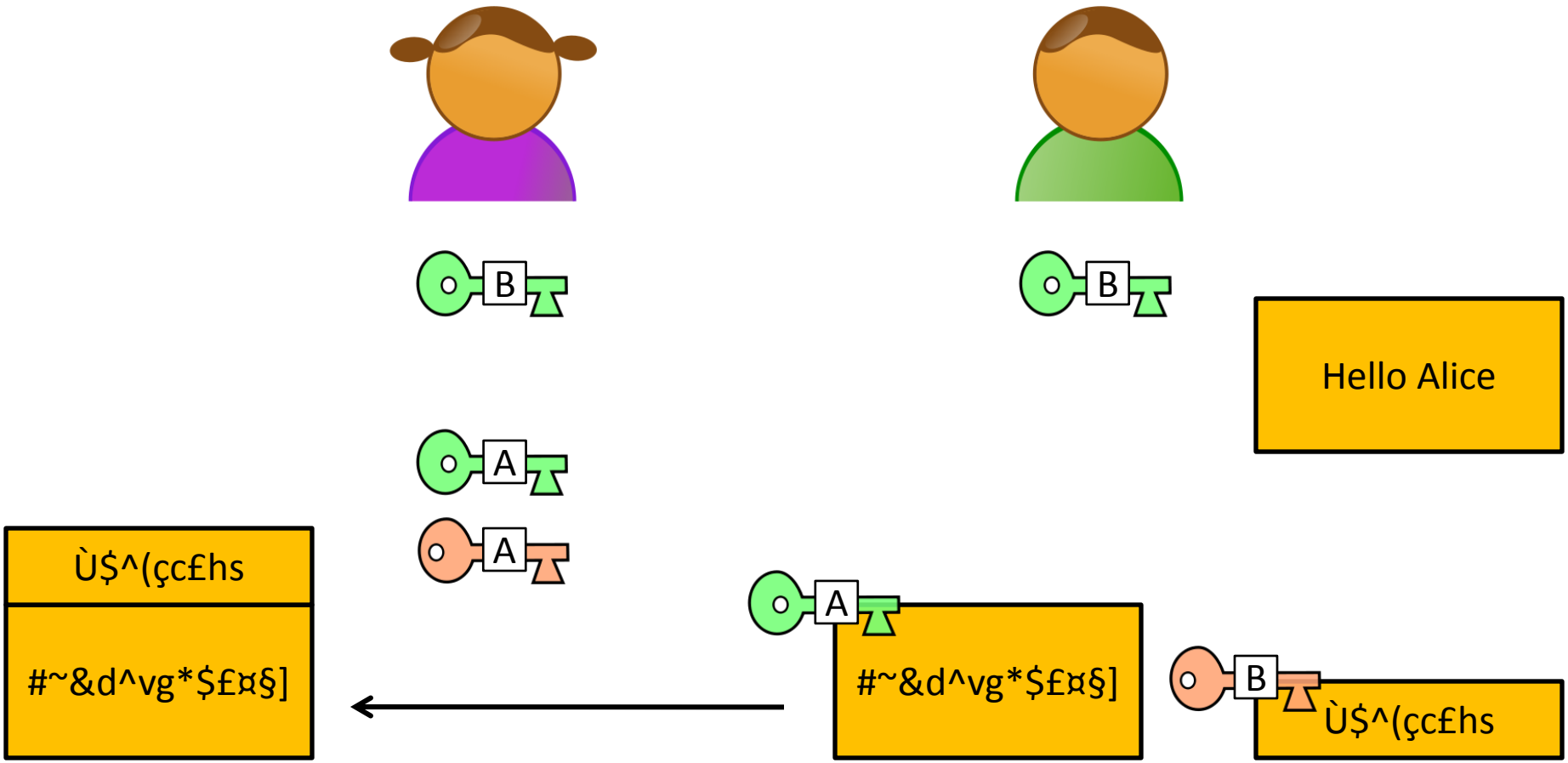




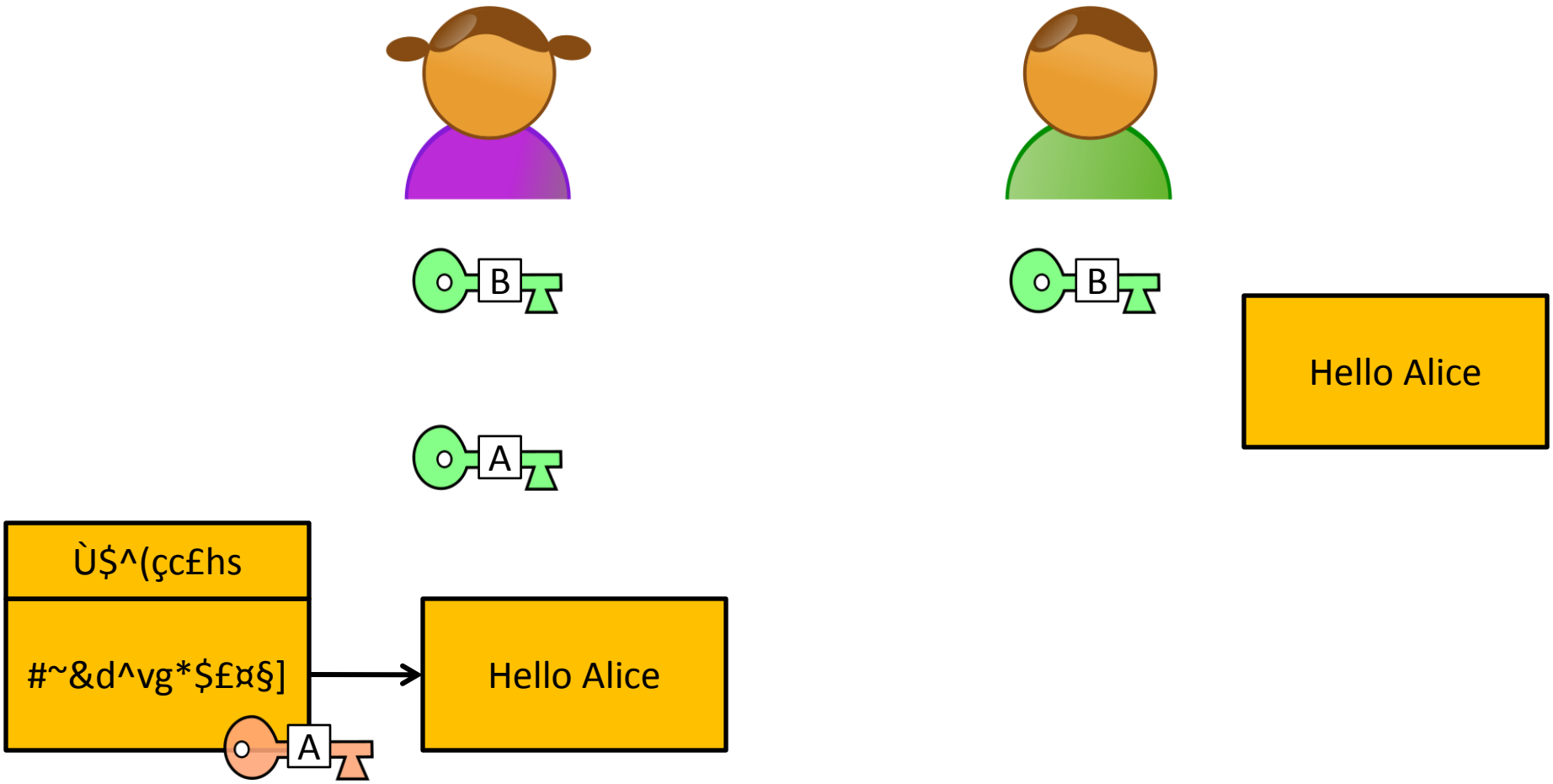
4) Bob chiffre son message avec la clé publique d'Alice.



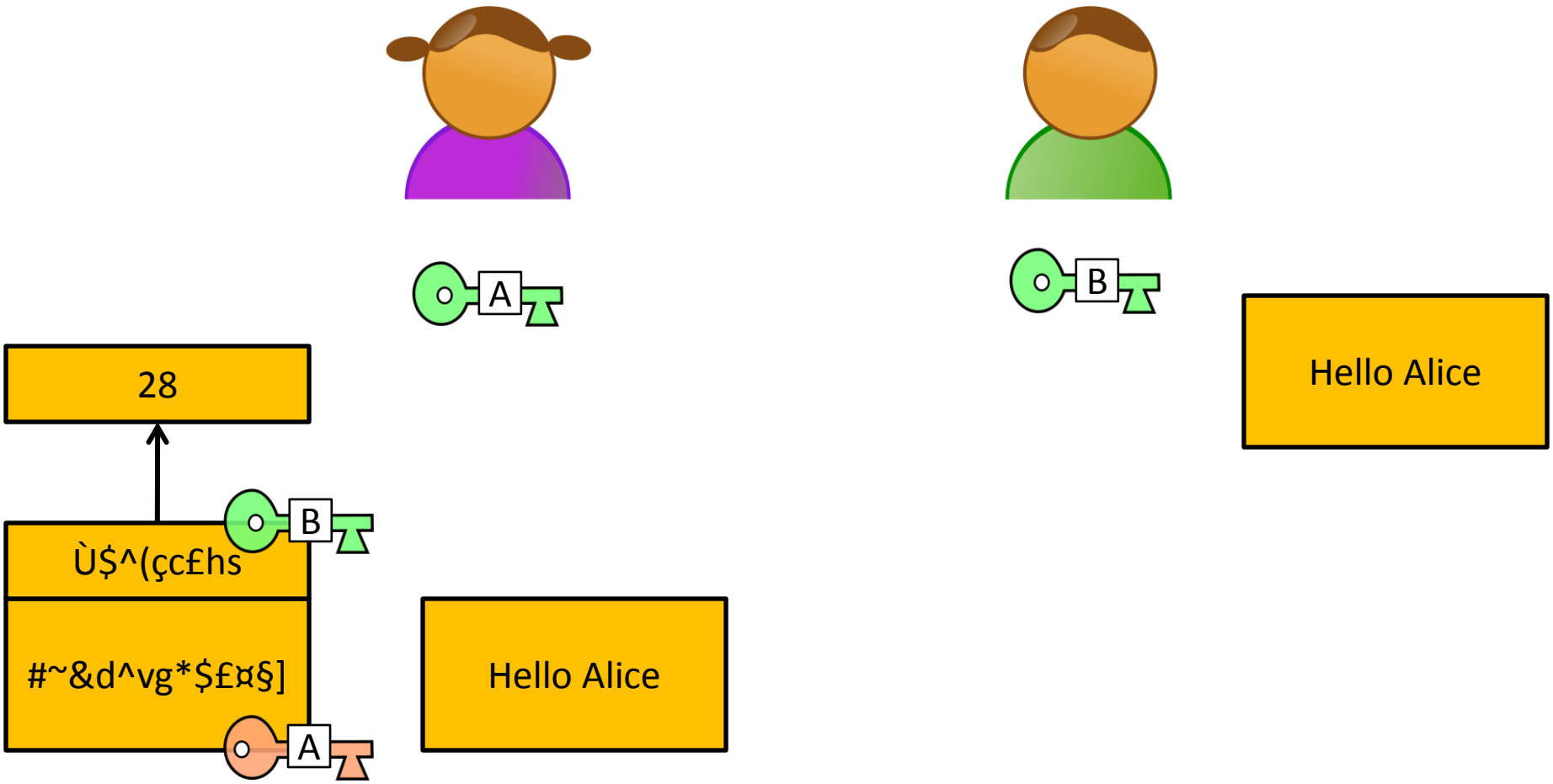
5) Bob envoie le message chiffré accompagné du condensat chiffré.



6) Alice déchiffre le message avec sa propre clé privée. À ce stade le message est lisible mais elle ne peut pas être sûre que Bob en est l'expéditeur.



7) Alice déchiffre le condensat avec la clé publique de Bob. A ce stade elle est sûre que le condensat viens de Bob.



8) Alice utilise la même fonction de hachage sur le texte en clair et compare avec le condensat déchiffré de Bob. Si les deux condensats correspondent, alors Alice peut avoir la certitude que Bob est l'expéditeur. Dans le cas contraire, on peut présumer qu'une personne malveillante a tenté d'envoyer un message à Alice en se faisant passer pour Bob !