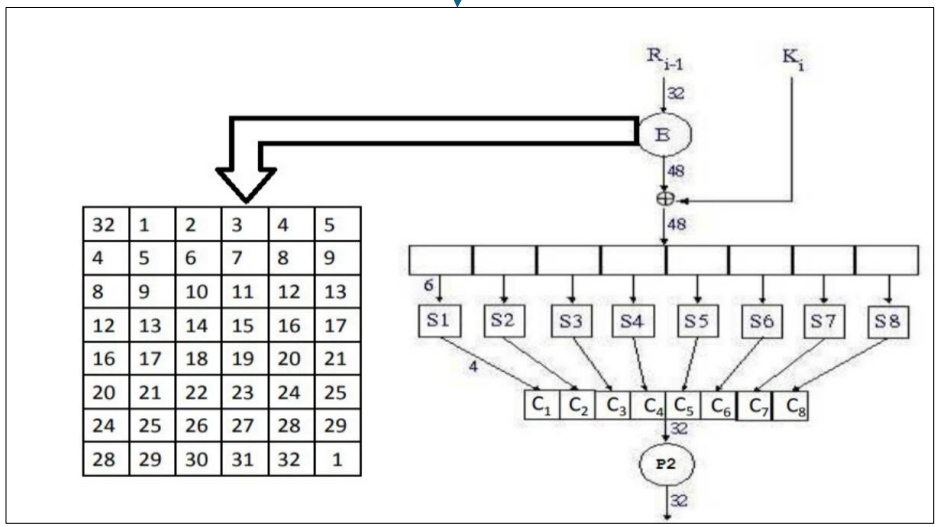
Cryptographie appliquée

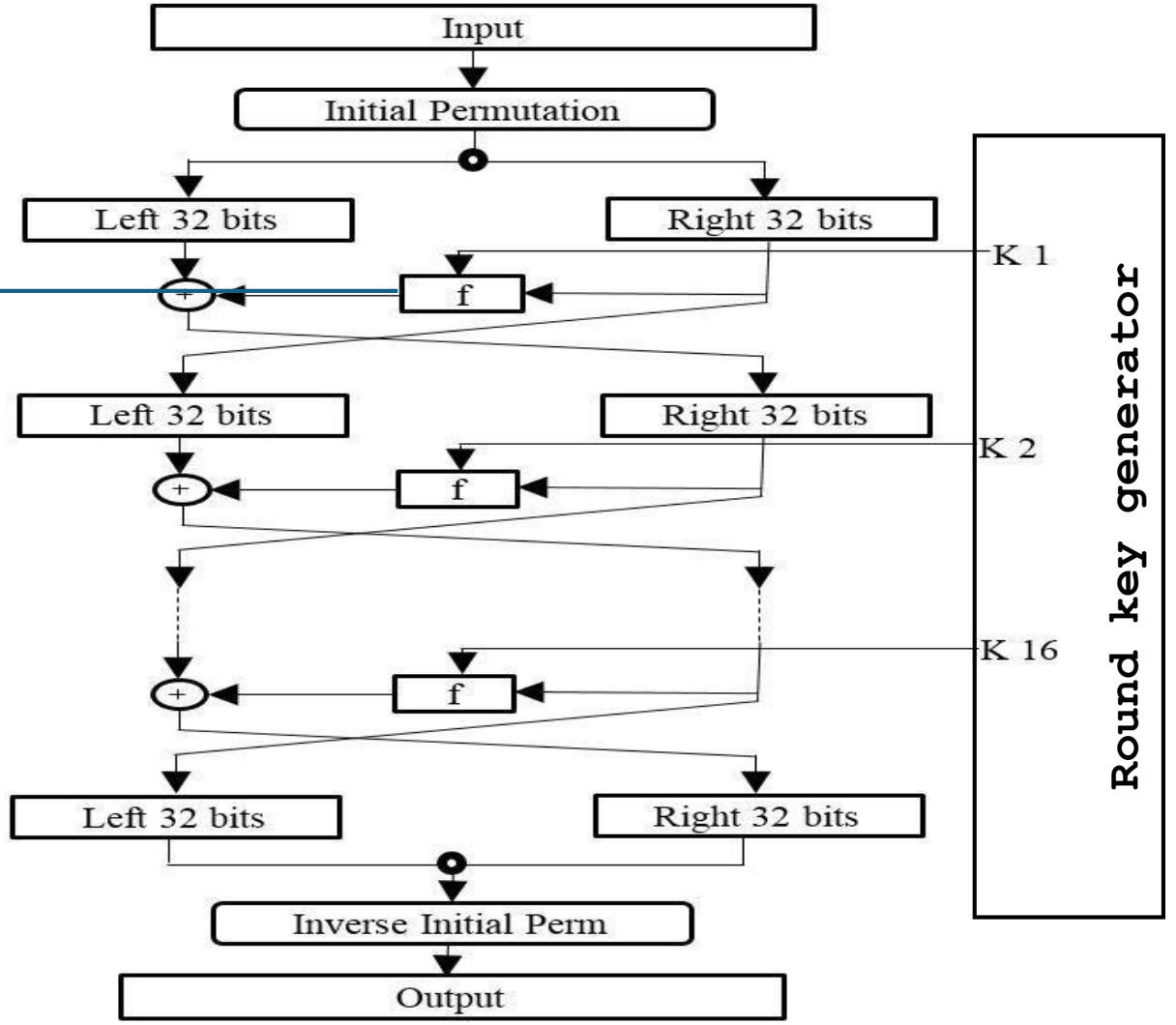
Pr. Hasnae L'AMRANI

Filière : Sécurité IT
&
confiance numérique

Cryptographie Asymétrique

Rappel : Chiffrement Symétrique





Cryptographie Symétrique: Avantages et inconvénients

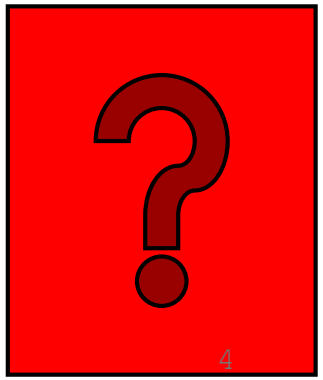
Avantage :

- Rapidité

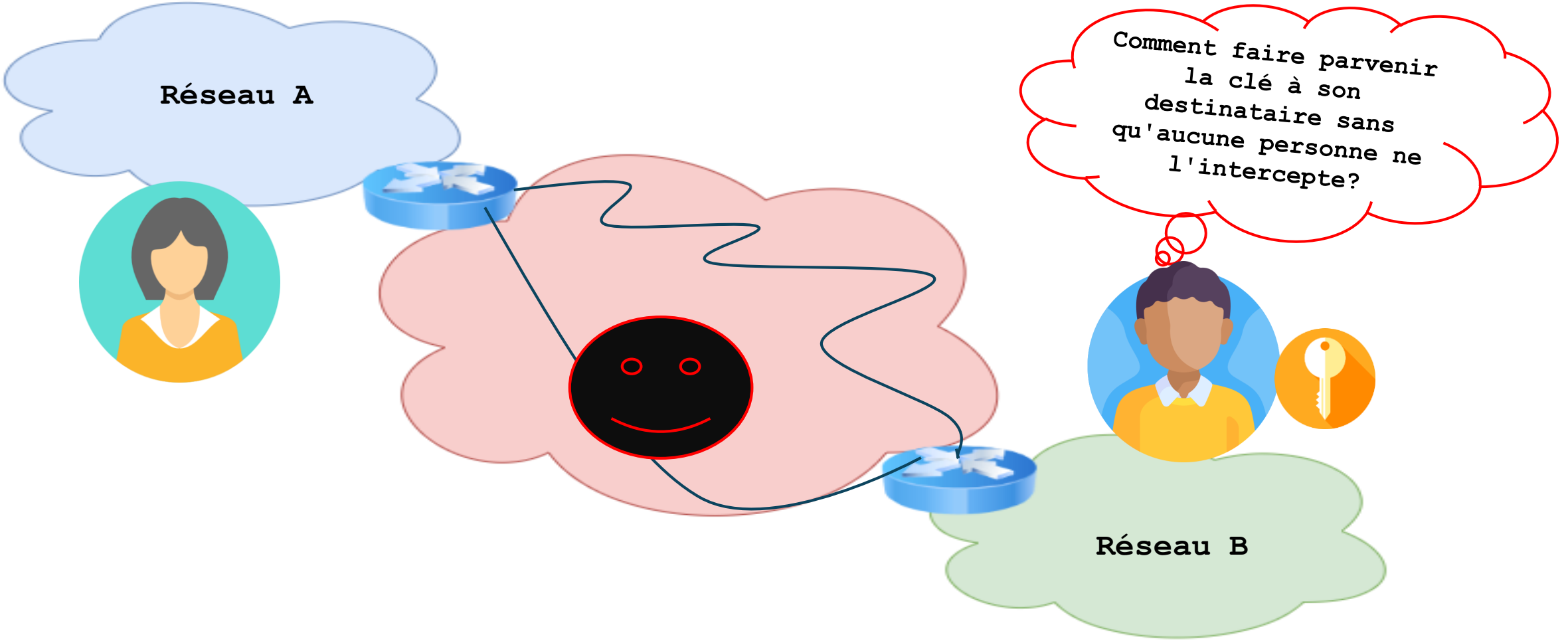
Inconvénients :

- La distribution des clés reste le problème majeur du cryptage Symétrique surtout lorsque Le nombre de communicants devient grand.

Comment faire parvenir la clé à son destinataire sans qu'aucune personne ne l'intercepte?



Cryptographie Symétrique: Avantages et inconvénients

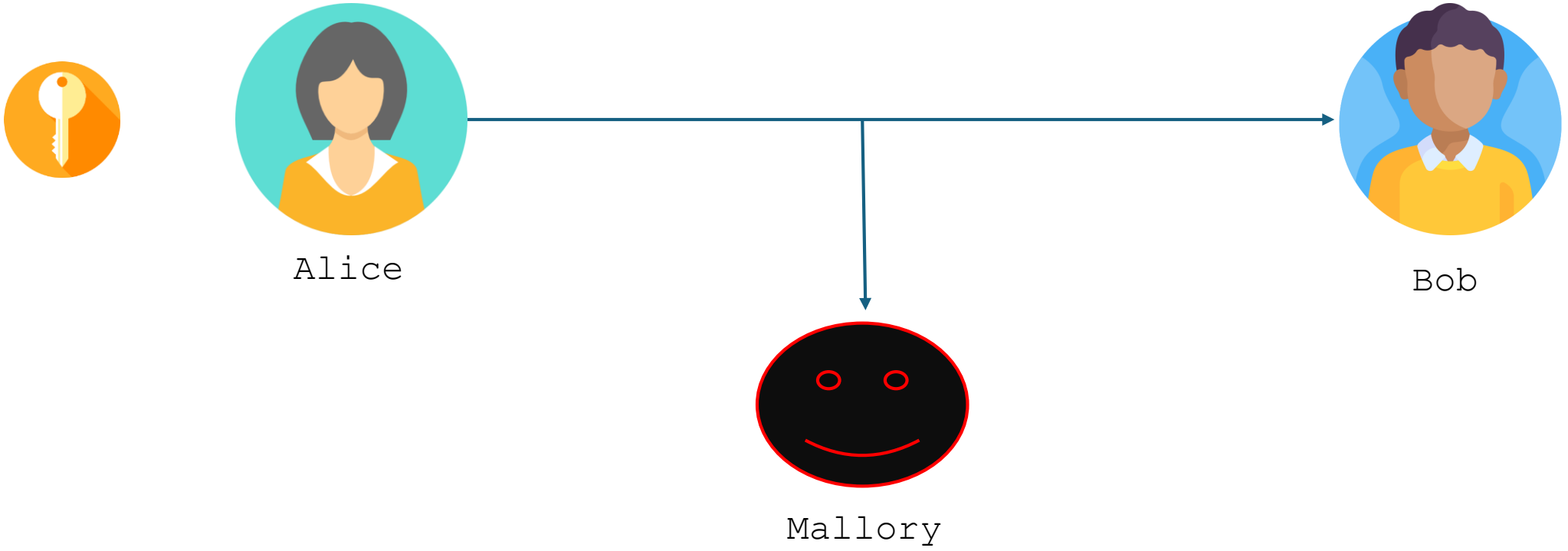


Cryptographie Symétrique: Solution

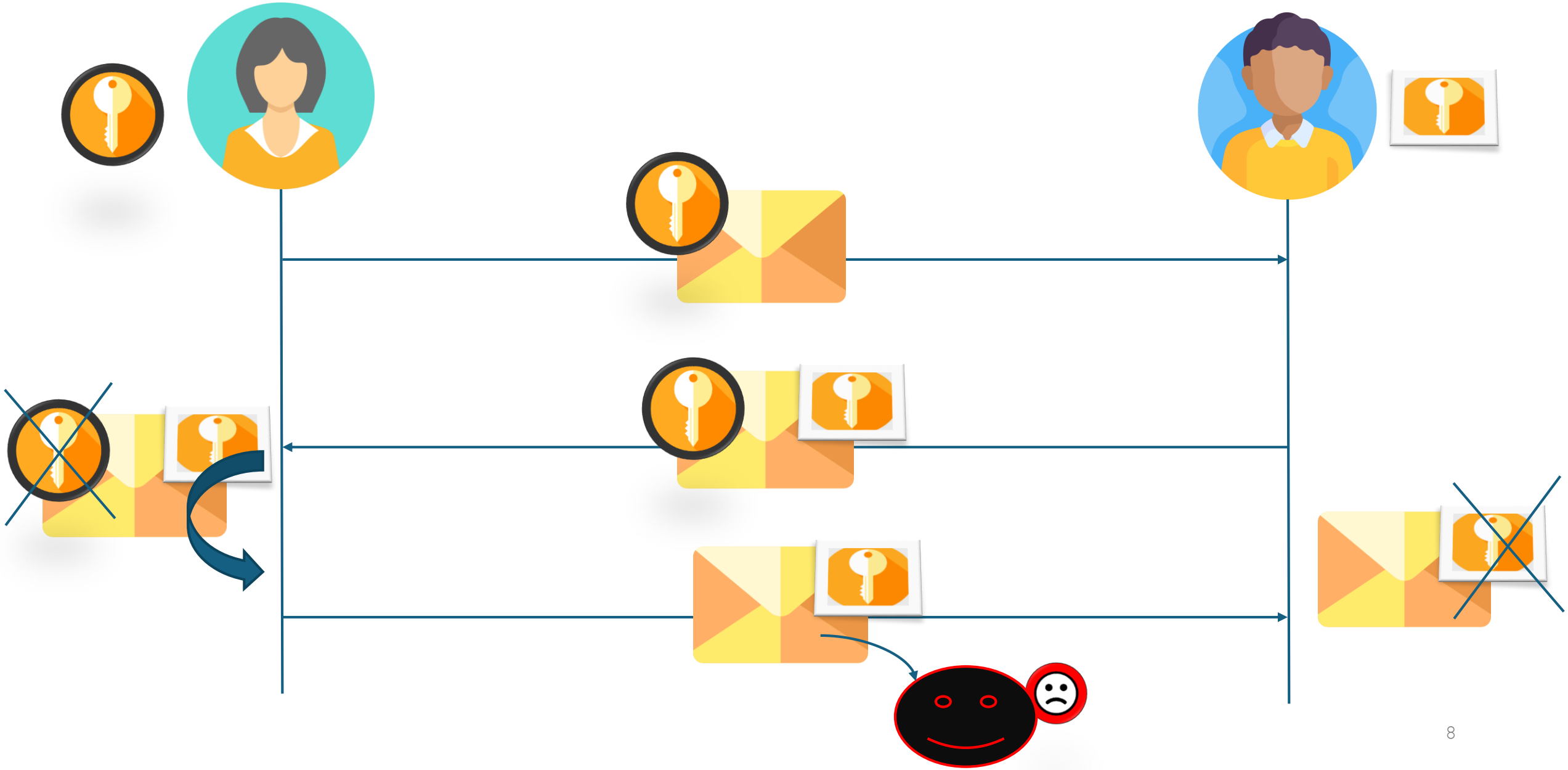
Comment cet homme peut-il traverser la rivière avec tous ses animaux ?

Cryptographie Symétrique: Solution

Comment faire parvenir la clé de Alice à Bob sans que Mallory l'intercepte?



Cryptographie Symétrique: Solution



Cryptographie Symétrique: Problème?

- L'ordre dans lequel sont effectués les chiffrements et les déchiffrements successifs joue un rôle crucial.
- Le flux échangé est important, inacceptable lors de l’échange des donnée de masse (exemple 1Go)
- De plus les échanges ne peuvent se faire qu'en présence de deux parties.

De là va apparaître la cryptographie asymétrique (à clé publique)

Cryptographie Asymétrique

Chaque entité possède **une paire de clés :**

Une clé publique

- **Connue** par toutes les autres entités;
- Utilisée pour **chiffrer** un message donné;

Une clé privée

- Qui **ne doit être connue** que par l'entité qui possède la paire en question;
- Utilisée pour **déchiffrer** un message;

Un message chiffré avec une clé publique ne peut être déchiffré qu'avec la clé privée correspondante.

Cryptographie Asymétrique

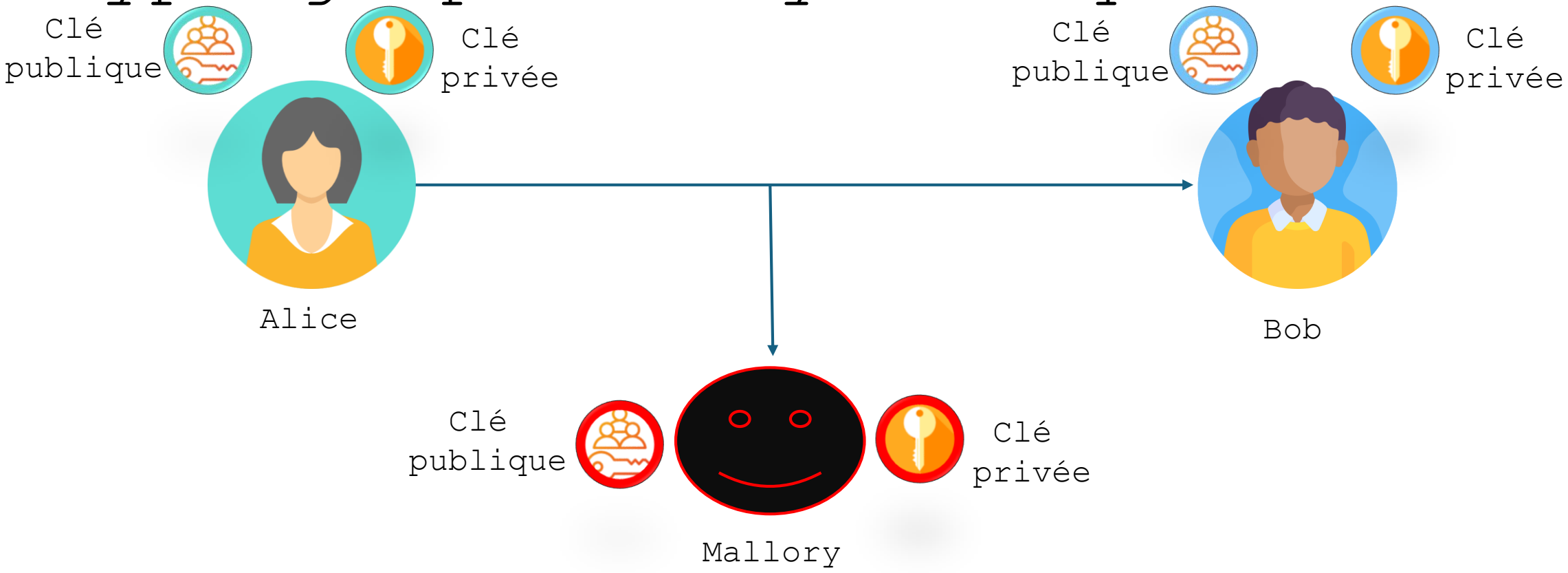
Clé publique

Donnée à tout le monde

Clé privée

Gardée confidentielle à sa possession

Cryptographie Asymétrique



- **Bob laisse sa clé public en libre accès.**
- **Alice peut à tout moment prendre la clé public et envoyer un message chiffré avec cette clé à Bob.**
- **Bob peut facilement déchiffrer le message avec sa clé privé**

Cryptographie Asymétrique

Difficulté :

- Il faut avoir un système de cryptage ayant des clés ke et kd différentes.

Objectif:

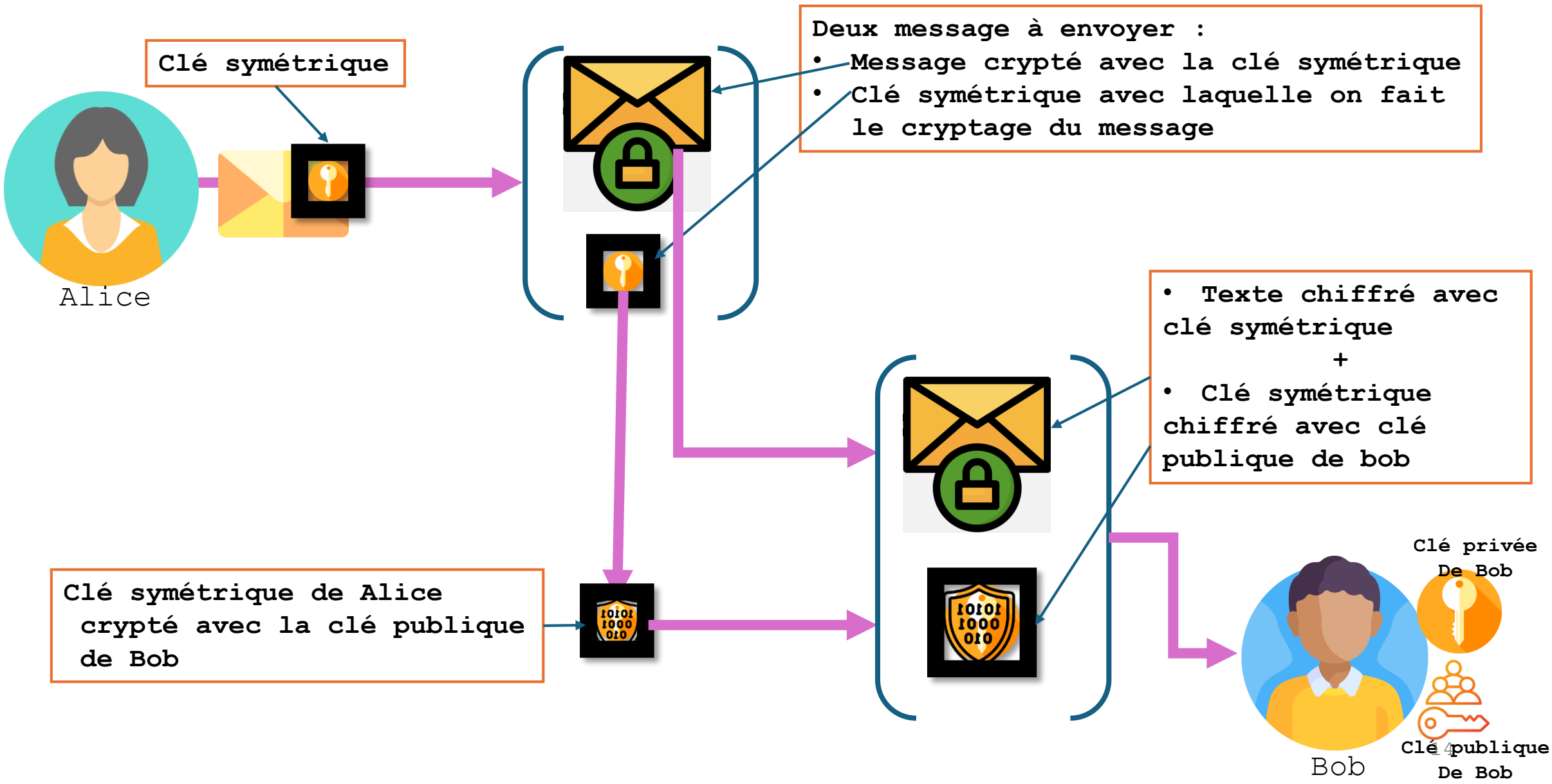
- Trouver des fonctions mathématiques faciles à utiliser dans un sens
- Très difficile à inverser

Problème:

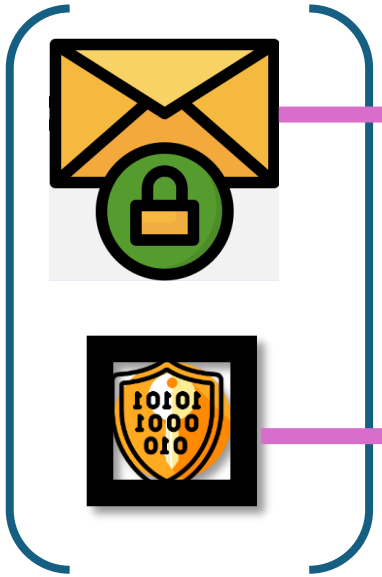
Très gourmand en calcul surtout avec un grand message à chiffrer!!! 1900 fois plus lent que AES.

Solution:
Le chiffrement asymétrique est utilisé pour distribuer des clés symétriques.

Cryptographie Hybride

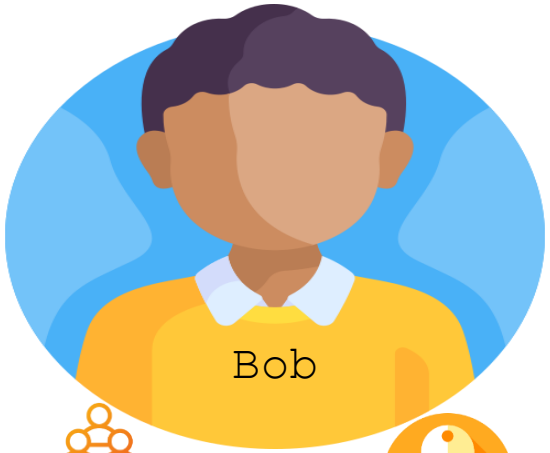


Cryptographie Hybride



Déchiffre le message chiffré avec la clé symétrique de Alice

Déchiffre la clé Symétrique De Alice avec sa propre clé privé



Clé publique De Bob

Clé privée De Bob

Cryptographie Asymétrique

- L'exponentiation de grands nombres premiers (**RSA)**
- Le problème des logarithmes discrets (**ElGamal**)
- Le problème du sac à dos (**Merkle-Hellman)**

RSA : Rivest-Shamir-Adleman

RSA : Rivest–Shamir–Adleman

- Basé sur :
  - Clé publique
  - Clé privée
- Génération des clés
- Algorithme RSA
  - Cryptage
  - Décryptage

RSA : Fonctionnement

1) Alice choisit deux grands nombres premiers **p** et **q** et calcule :

- **Le module de chiffrement c'est** $n = pxq$
- **L'indicatrice d'Euler c'est** $\varphi(n) = (p - 1)(q - 1)$

2) Alice choisit un entier **e** qui n'a pas de facteur commun avec $\varphi(n)$ **(premiers entre eux)** et **strictement inférieur à** $\varphi(n)$, appelé **exposant de chiffrement :** $1 < e < \varphi(n)$

3) Alice calcule **d** tel que **(ed-1)** est exactement divisible par $\varphi(n)$.

- $ed \equiv 1 \pmod{\varphi(n)}$

4) Elle déduit :

- **Clé publique = (n,e)**
- **Clé privée =(n,d)**

RSA : Fonctionnement

- Grâce à la **clé public** d'Alice, Bob peut **chiffrer** son message avec la formule **RSA.**
- Il ne peut plus le **déchiffrer**, car RSA est **impossible à inverser**, à **moins de connaître p et q**.
- Alice reçoit le message **chiffré** de Bob et peut le **déchiffrer** grâce **à p et q**.

Bob veut envoyer un message **m** à Alice :

Chiffrement : $c = m^e \bmod n$

Alice reçoit le message **c** et calcule :

Déchiffrement : $m = c^d \bmod n = (m^e \bmod n)^d \bmod n$

RSA : Exemple

Soit **p=5, q=7, m=12**

- **p=5, q=7, donc n=p*q=35 et φ(n)=(p-1)*(q-1)=24**
- Alice choisit e=5 : clé publique (5,35)
- déduisez le d =? : clé privé : (d,35)
- Bob: (chiffrement) : **m=12, c = m^e mod n ,C = 12^5 mod 35 , C=17**
- Alice: (déchiffrement) : **c=17, m = c^d mod n = 17^d mod 35**

RSA : Exemple

Nous devons maintenant calculer d d en résolvant l'équation :

$$e \times d \equiv 1 \bmod \phi(n)$$

Autrement dit, trouver l'inverse modulaire de :

$$e=5 \bmod \phi(n)=24$$

<u>Étape 1 : Appliquer l'algorithme d'Euclide pour trouver le PGCD</u>

Il faut trouver le PGCD de e = 5 et ϕ (n) = 24

$$24=4\times5+4$$
$$5=1\times4+1$$
$$4=4\times1+0$$

(Le reste est 0, donc le PGCD est 1).

RSA : Exemple

Étape 2 : Remonter dans les équations pour trouver d

Maintenant que nous avons trouvé le PGCD 1, nous allons remonter dans les équations pour exprimer 1 comme une combinaison linéaire de 5 et 24.

$$5=1\times4+1 \rightarrow 1=5-1\times4$$

$$24=4\times5+4 \rightarrow 4=24-4\times5$$

Remplacer 4 par 24−4×5 (de la première division) :

$$1=5-1\times(24-4\times5)$$

$$1=5-1\times24+4\times5$$

$$1=5\times5-1\times24$$

Cela signifie que d=5

L'inverse modulaire de $e = 5 \bmod \phi(n) = 24$ est $d = 5$

RSA : Exemple

p=5, q=7, m=12

n=p*q=35 et φ(n)=(p-1)*(q-1)=24

e=5, d= 5

Chiffrement : $c = m^e \bmod n = 12^5 \bmod 35 = 248,832 \bmod 35 = 17$

Déchiffrement : $m = c^d \bmod n = 17^5 \bmod 35 = 1,419,857 \bmod 35 = 12$

Exercice 1

Soit le système RSA suivant :

$p = 3,\ q = 11\ ,\ n = p \times q = 33$

$\phi\ (\ n\ ) = (\ p - 1\ ) \times (\ q - 1\ )$

$= (\ 3 - 1\ ) \times (\ 11 - 1\ ) = 20$

e = 7(exposant public choisi tel que e et $\phi(n)$ soient premiers entre eux).

Étape 1 : Calcule l'exposant privé d d en utilisant l'algorithme d'Euclide étendu pour résoudre $e \times d \equiv 1 \mod \phi(n)$.

Étape 2 : Chiffre le message M=7 en utilisant la formule de chiffrement : $c = m^e \mod n$

Étape 3 : Déchiffre le message chiffré C en utilisant la formule de déchiffrement : $m = c^d \mod n$

Exercice 2

Soit le système RSA suivant :

$p = 3,\ q = 11\ ,\ n = p \times q = 33$

$\phi\ (\ n\ ) = (\ p - 1\ ) \times (\ q - 1\ )$

$= (\ 3 - 1\ ) \times (\ 11 - 1\ ) = 20$

e = 3(exposant public choisi tel que e et $\phi(n)$ soient premiers entre eux).

Étape 1 : Calcule l'exposant privé d d en utilisant l'algorithme d'Euclide étendu pour résoudre $e \times d \equiv 1 \mod \phi(n)$.

Étape 2 : Chiffre le message M=7 en utilisant la formule de chiffrement : $c = m^e \mod n$

Étape 3 : Déchiffre le message chiffré C en utilisant la formule de déchiffrement : $m = c^d \mod n$