Cryptographie post quantique

Mélissa Rossi

Présentation

Prépa (2010-2013)

Lycée du Parc (Lyon)

Ecole d'ingénieur (2013-2015)

TELECOM ParisTech

Master de recherche (2015-2016)

ENS
ÉCOLE NORMALE SUPÉRIEURE

Stage (2016)

THALES

Pré-doc (2016-2017)

CRYPTOGRAPHY RESEARCH
a division of Rambus

Doctorat en cryptographie post quantique

Mai 2017 - 2020

Encadrement académique

Laboratoire de recherche
Direction des recherches
Projets de recherche par groupe

Encadrement industriel

Contrat cifre
Thèse à plein temps
Collaborations

Encadrement étatique

Un de mes directeurs de recherche est agent de l'état
Recherches plus appliquées de type attaques

Le monde de la recherche

Cryptographie : Entre les maths et l'informatique

Vie de labo

Beaucoup d'interactions entre chercheurs au labo (brouillons, tableaux blancs…)

Petites avancées régulières

Interactions à l'international

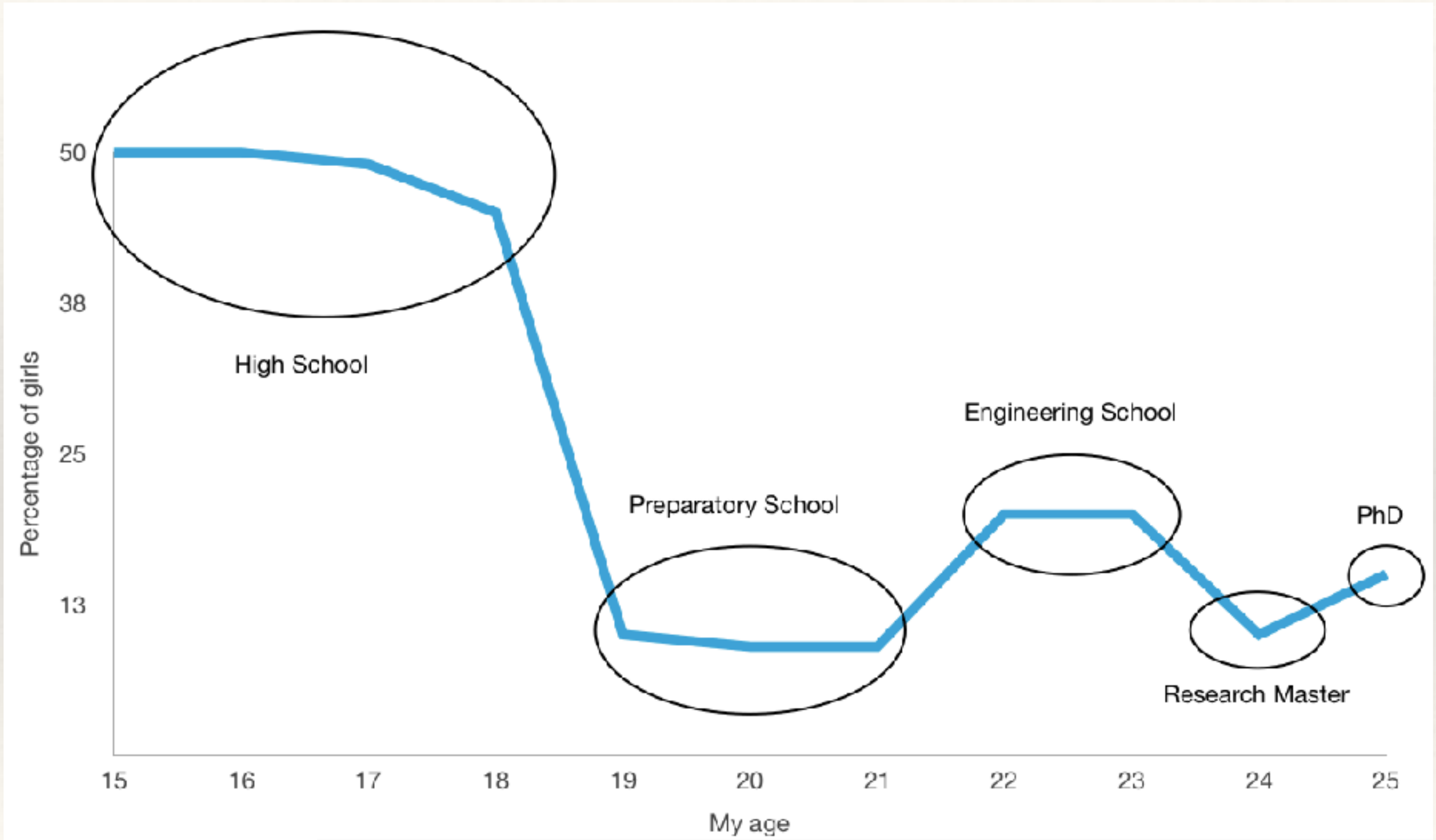
Compétitions d'attaques

Rédaction d'articles scientifiques à plusieurs

Conférences, workshops, retreats …

20% du temps à l'étranger

Pourcentage de filles pendant mon parcours



La recherche en général

Plus on avance dans la recherche, moins il y a de filles.

Les filles cryptologues sont extrêmement peu à avoir l'HDR en France

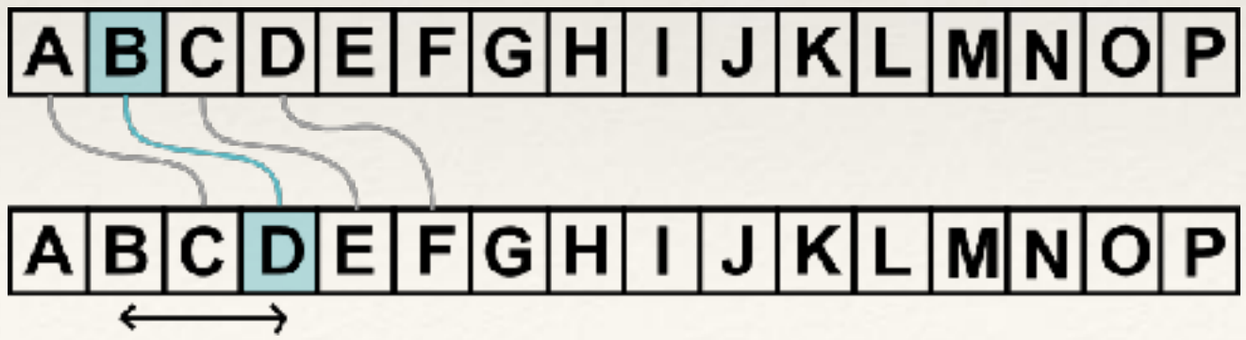
⟶ Responsabilité de votre génération

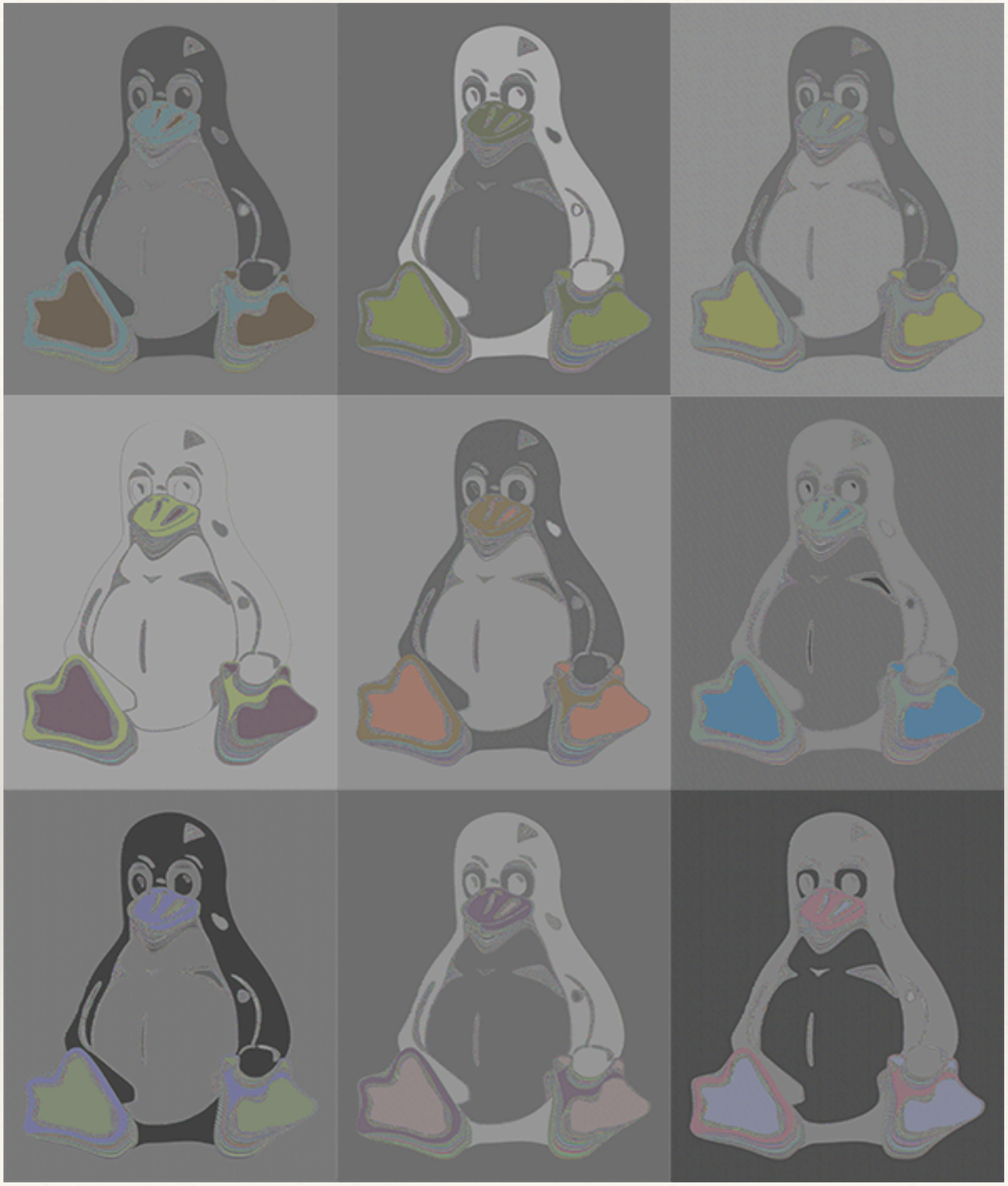
Cryptographie

Idée : envoyer des messages secrets

Idée des Spartiates

Chiffrement de césar





Enigma

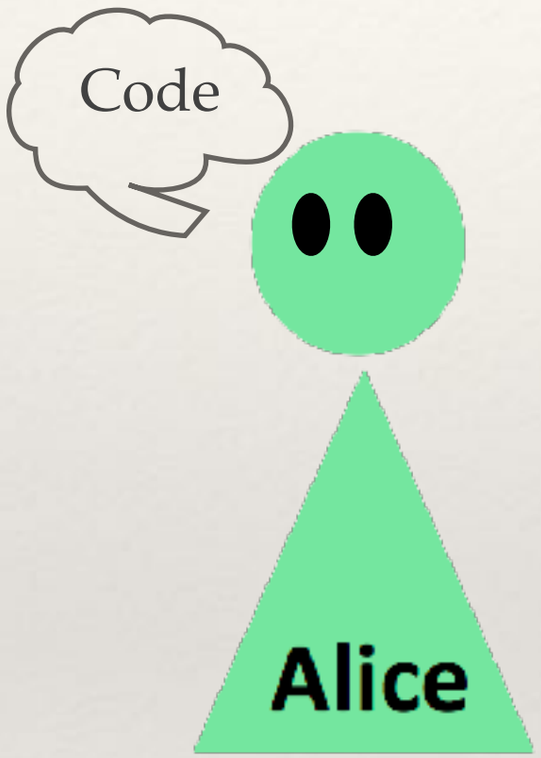
Principe de Kerckhoffs

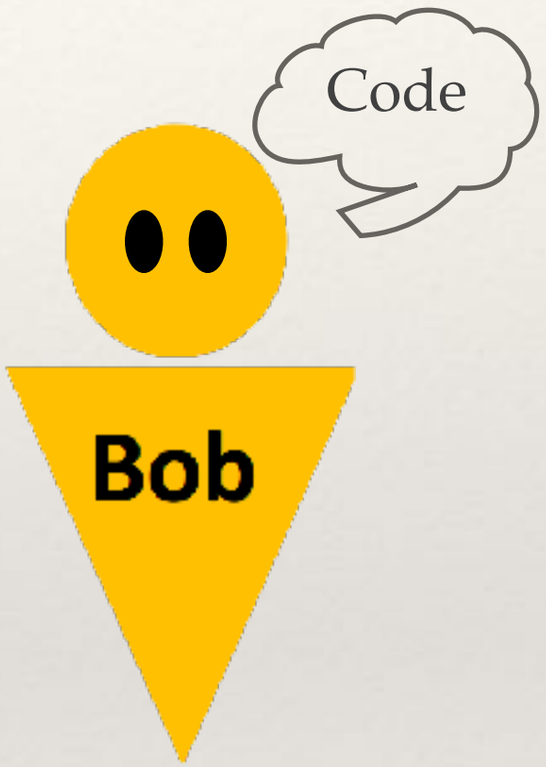
Axiomes fondamentaux de la cryptographie

Les détails des algorithmes de chiffrement doivent être publics

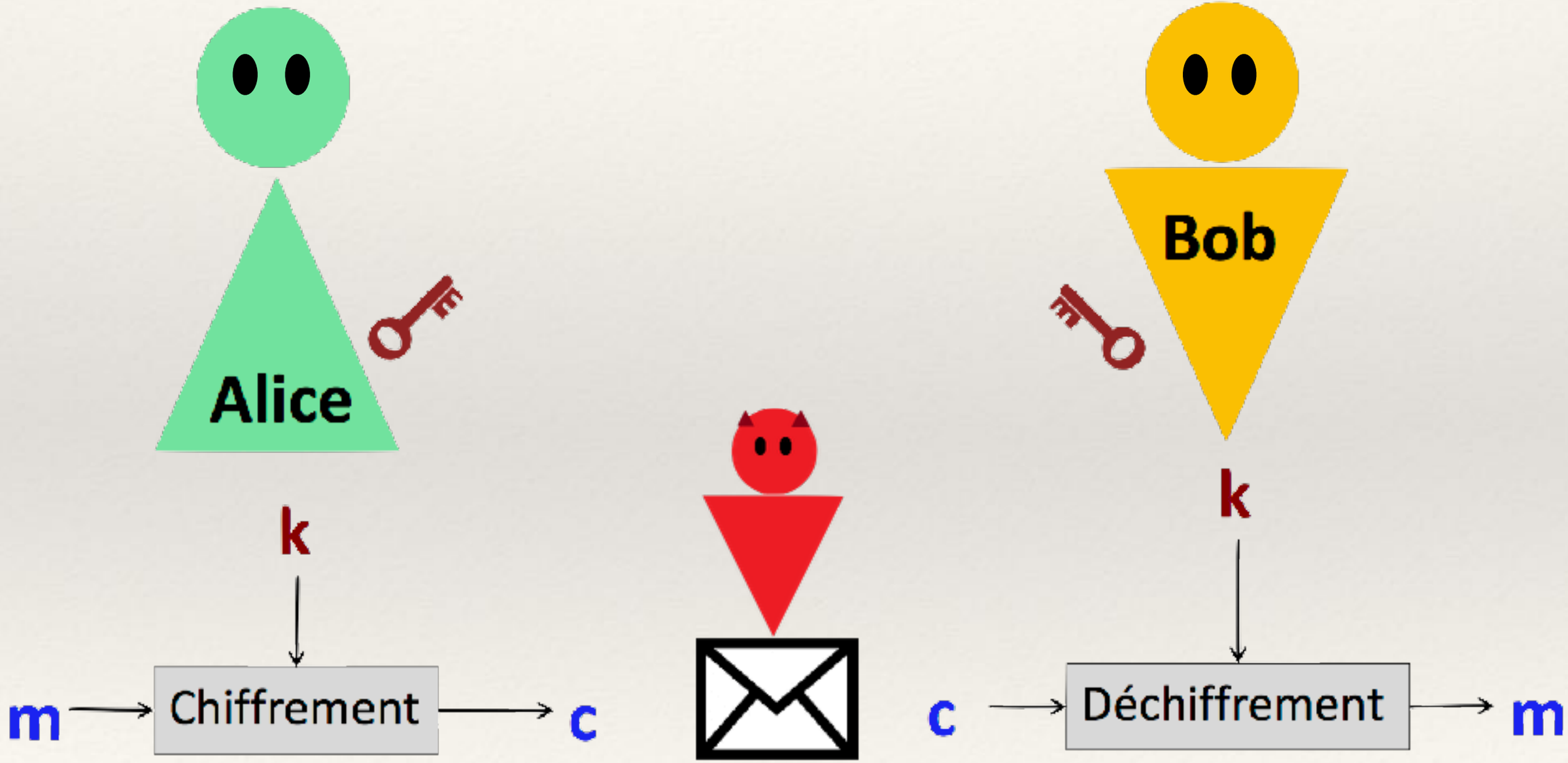
Il ne manque que la clé à l'ennemi
pour pouvoir déchiffrer.

Cryptographie symétrique



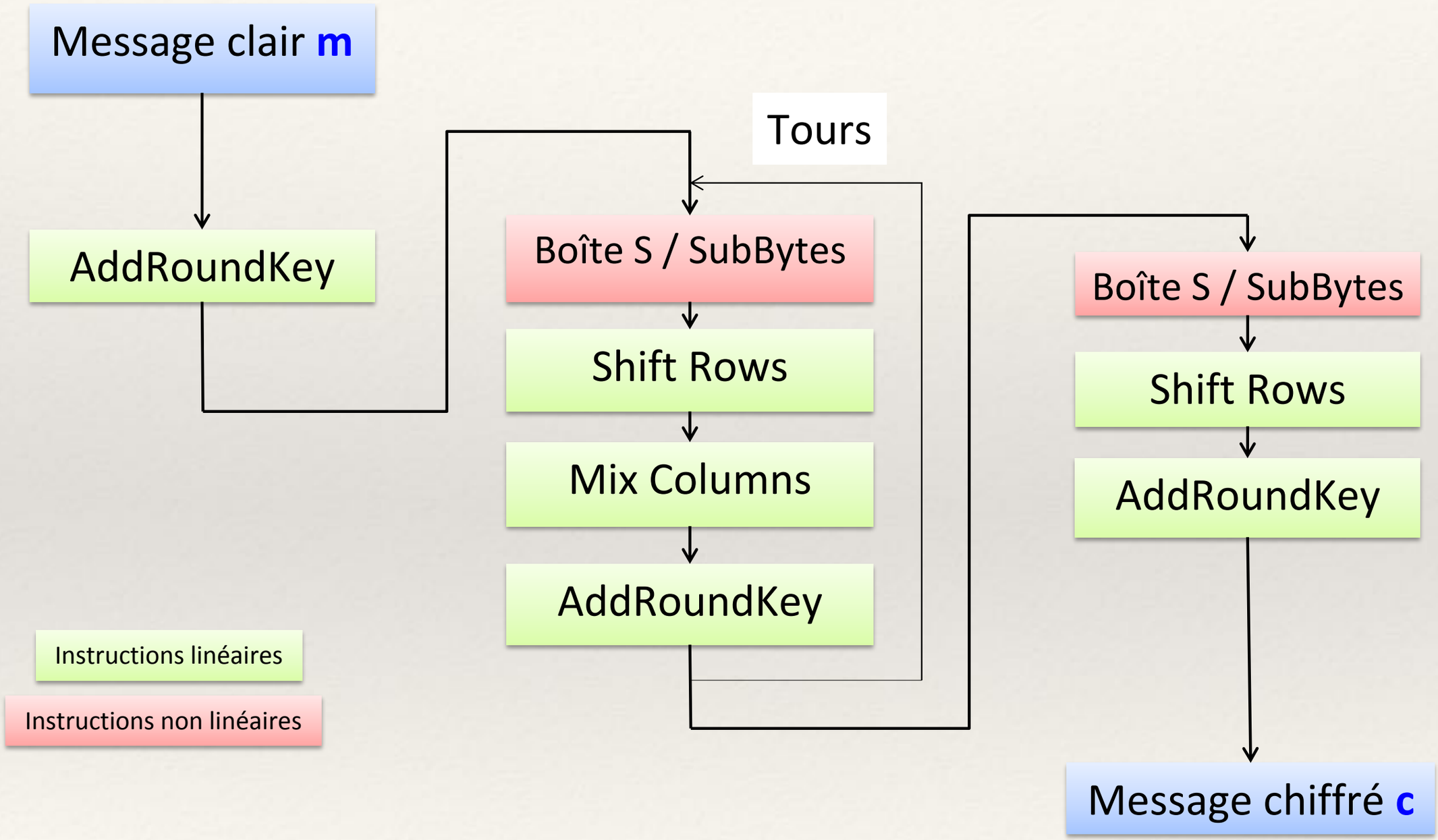


Cryptographie symétrique



AES

Suite à un concours en 2000



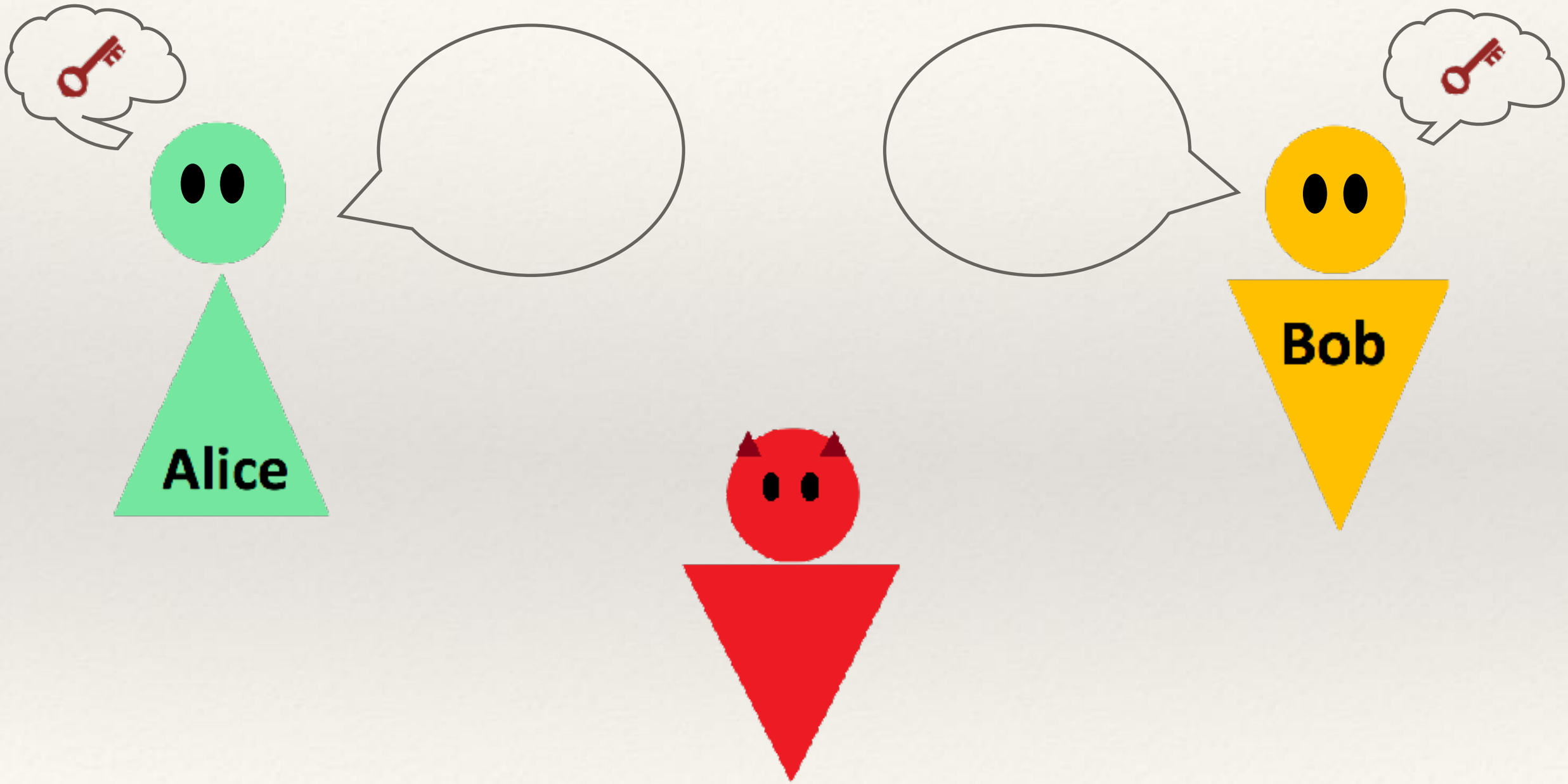
Cryptographie symétrique

- Les deux parties connaissent une clé secrète
- Chiffrement : Mélange de la clé et du message
- Déchiffrement : Opération inverse
- Standard utilisé : AES

Cryptographie asymétrique

Comment faire en sorte qu'Alice et Bob **aient une clé commune** ?

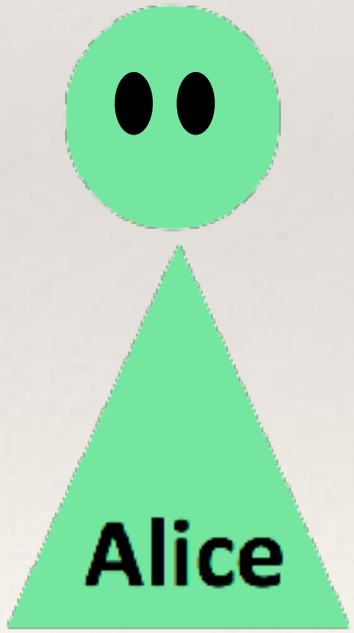
Cryptographie asymétrique



Idée de Merkle

Puzzle de Merkle : Enigme demandant un effort important mais pas hors de portée.
Exemple AES avec une clé de 20 bits

Temps T pour la résoudre
Une fois résolu, on obtient un entier i et une clé k

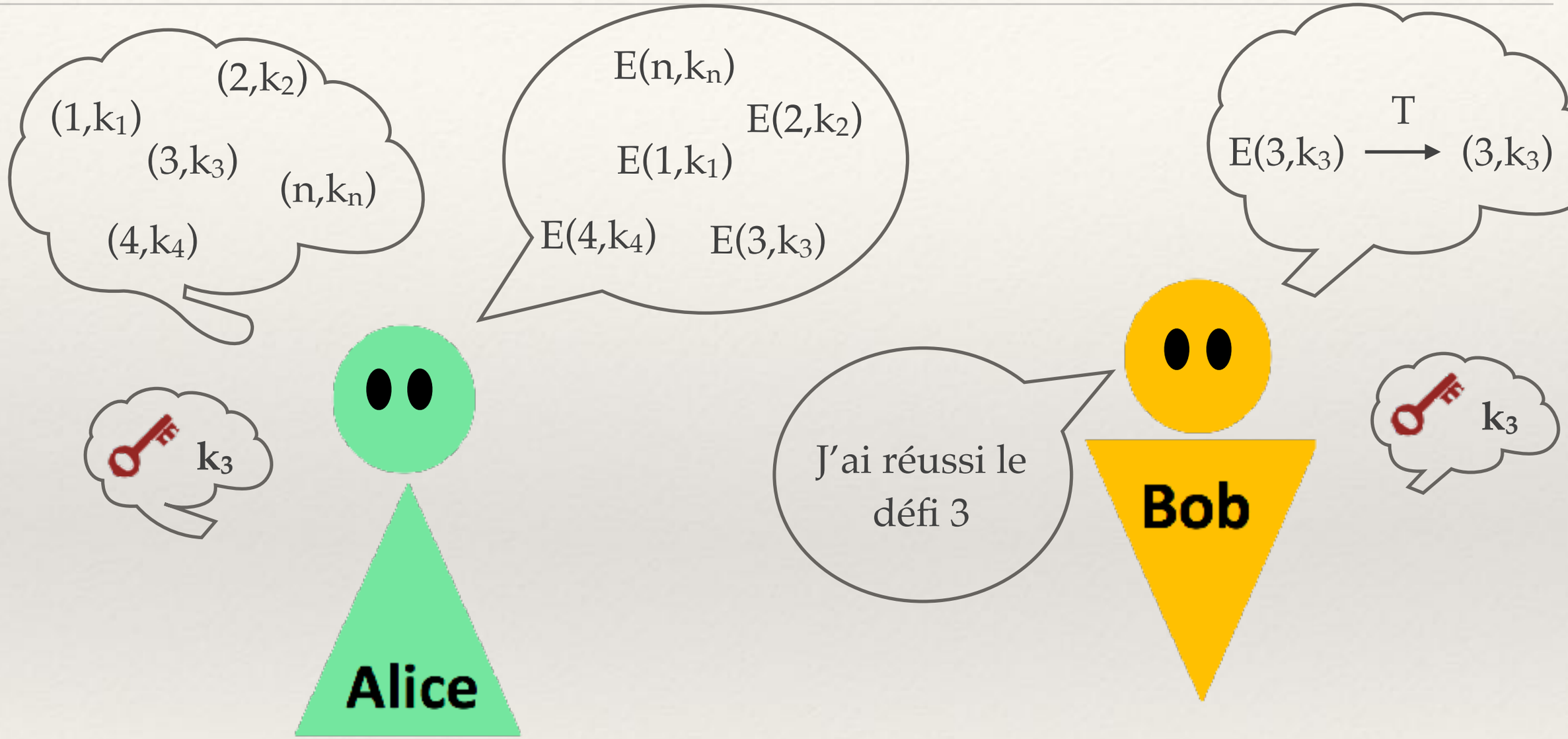


E(i,k)

$(1,k_1) \longrightarrow E(1,k_1)$
$(2,k_2) \longrightarrow E(2,k_2)$

$(n,k_n) \longrightarrow E(n,k_n)$

Idée de Merkle

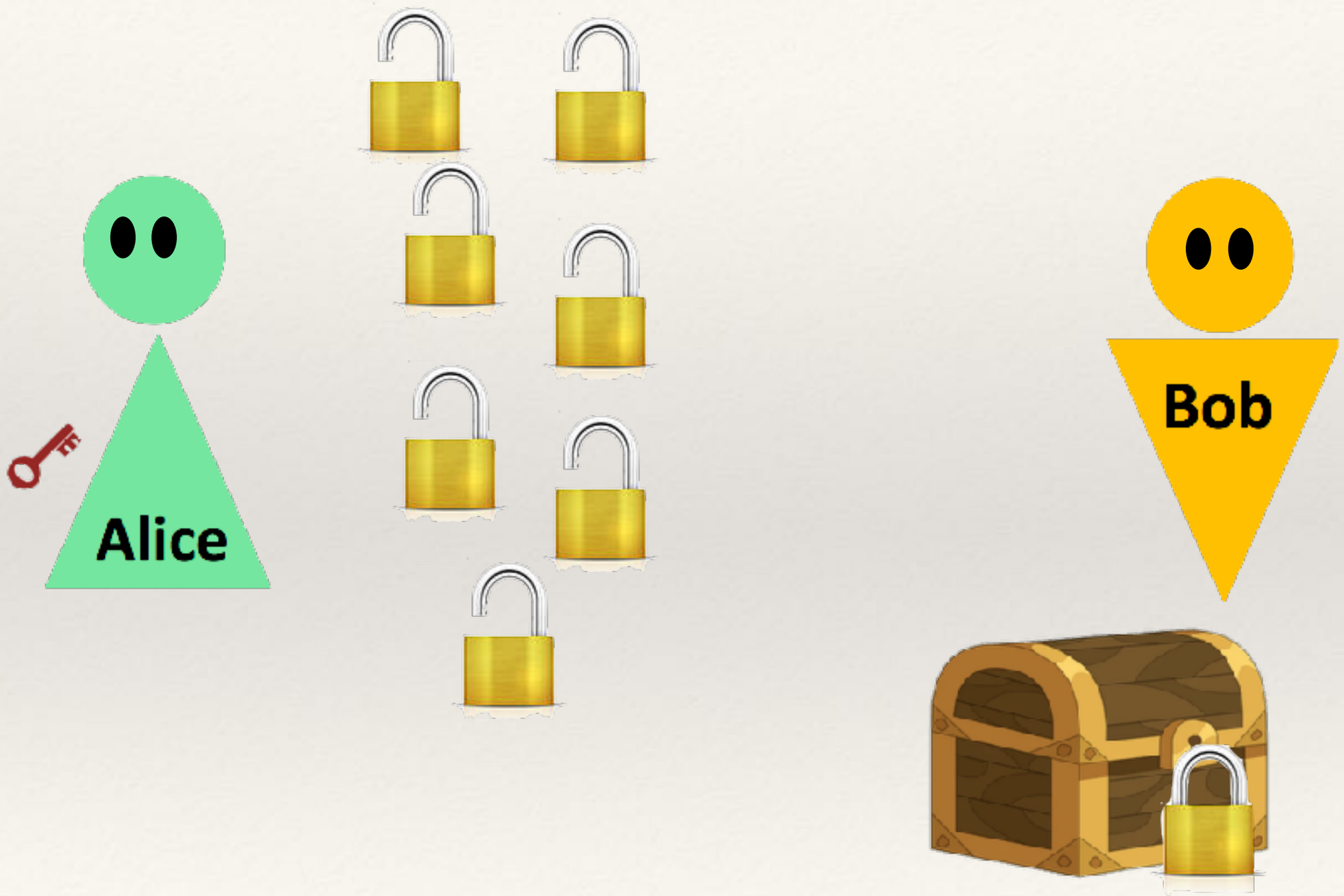


Eve est obligée de résoudre les n défis.
Et elle récupère celui où elle obtient 3

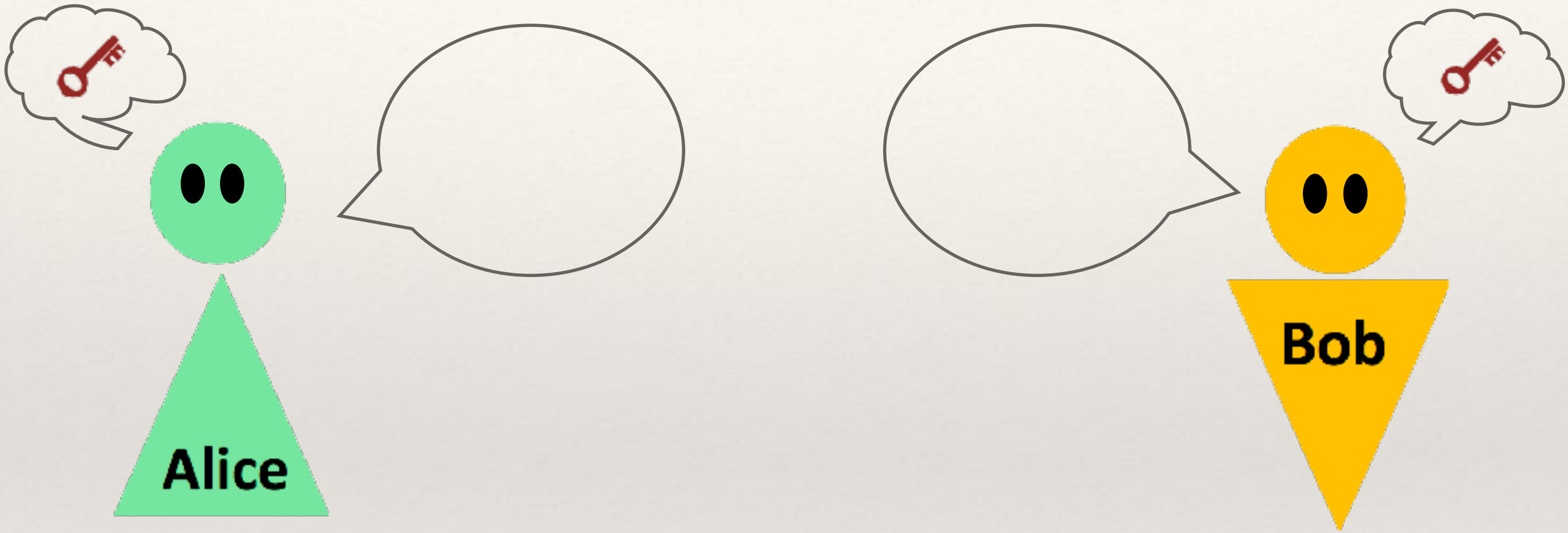
Puzzles de Merkle

Attaque : n/2 T en moyenne

Cryptographie asymétrique



Cryptographie asymétrique



- Protocole d'échanges qui aboutit à un secret commun
- **Hypothèses de sécurité** : limitation en temps de calcul de l'attaquant

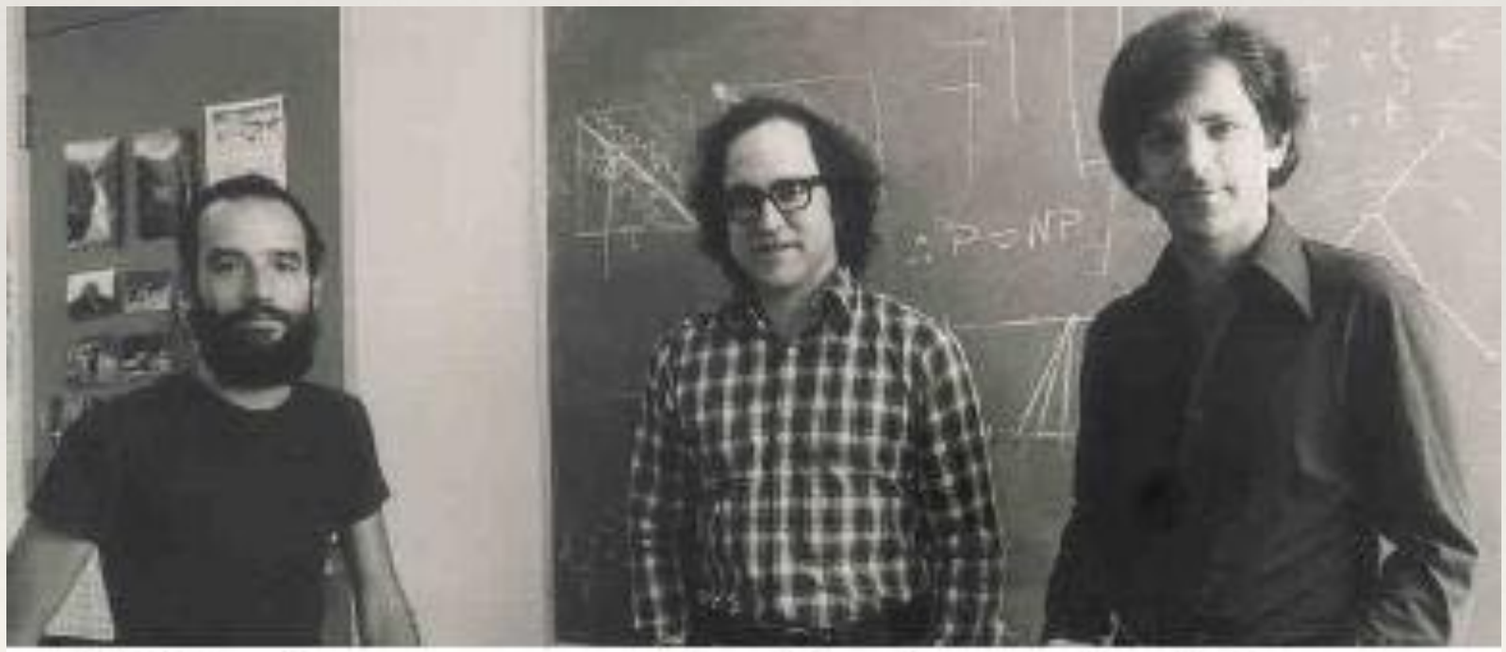
Hypothèse de la factorisation

Multiplier deux entiers

VS

Factoriser un entier

Idée utilisée dans RSA (années 70)



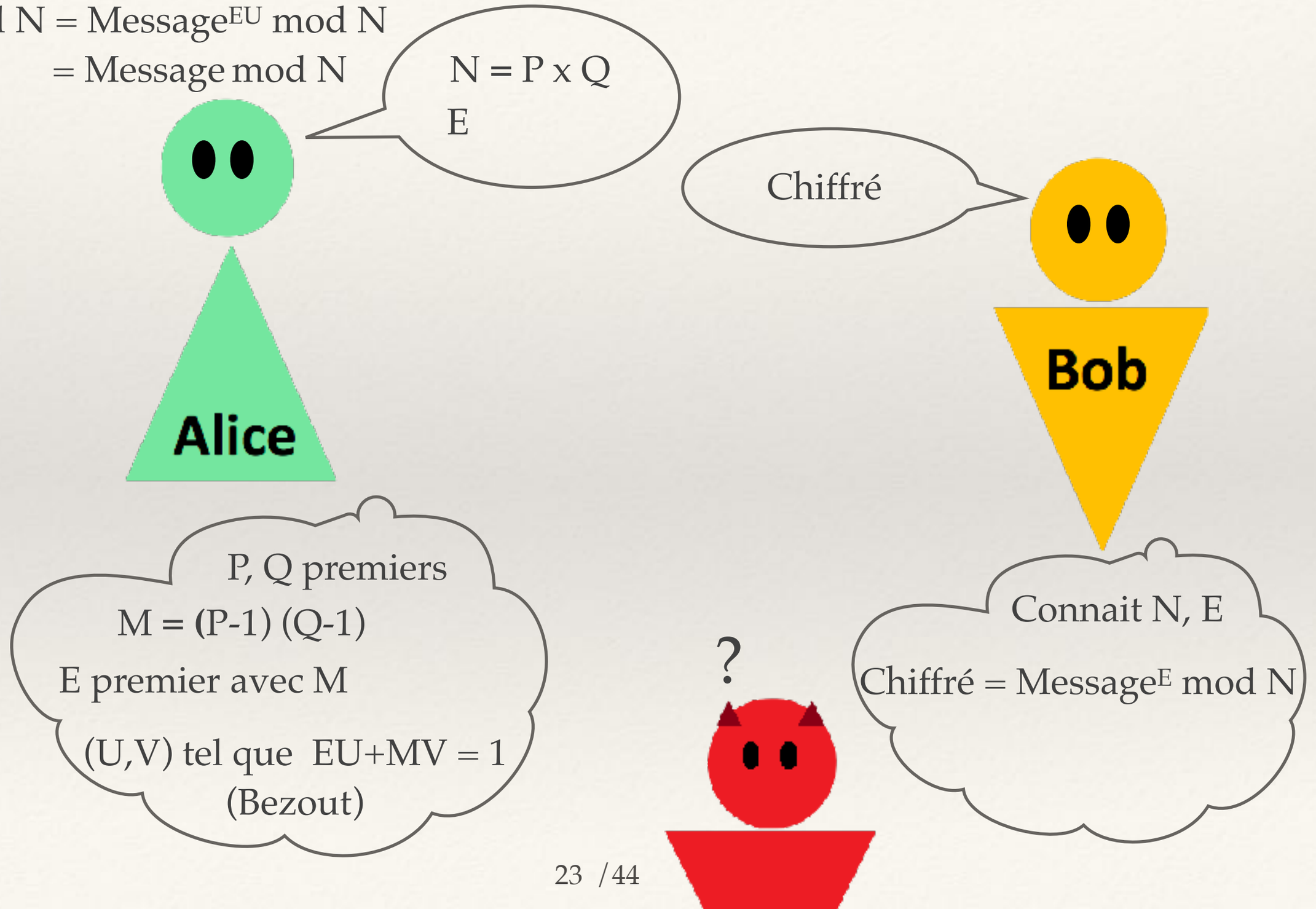
RSA

$x^{(P-1)(Q-1)} \bmod N = 1 \bmod N$

Th. d'Euler

$Chiffré^{U} \bmod N = Message^{EU} \bmod N$

$= Message \bmod N$



Hypothèse de du logarithme discret

$$y = x^a \bmod N$$

$$a = \ln_x(y)$$

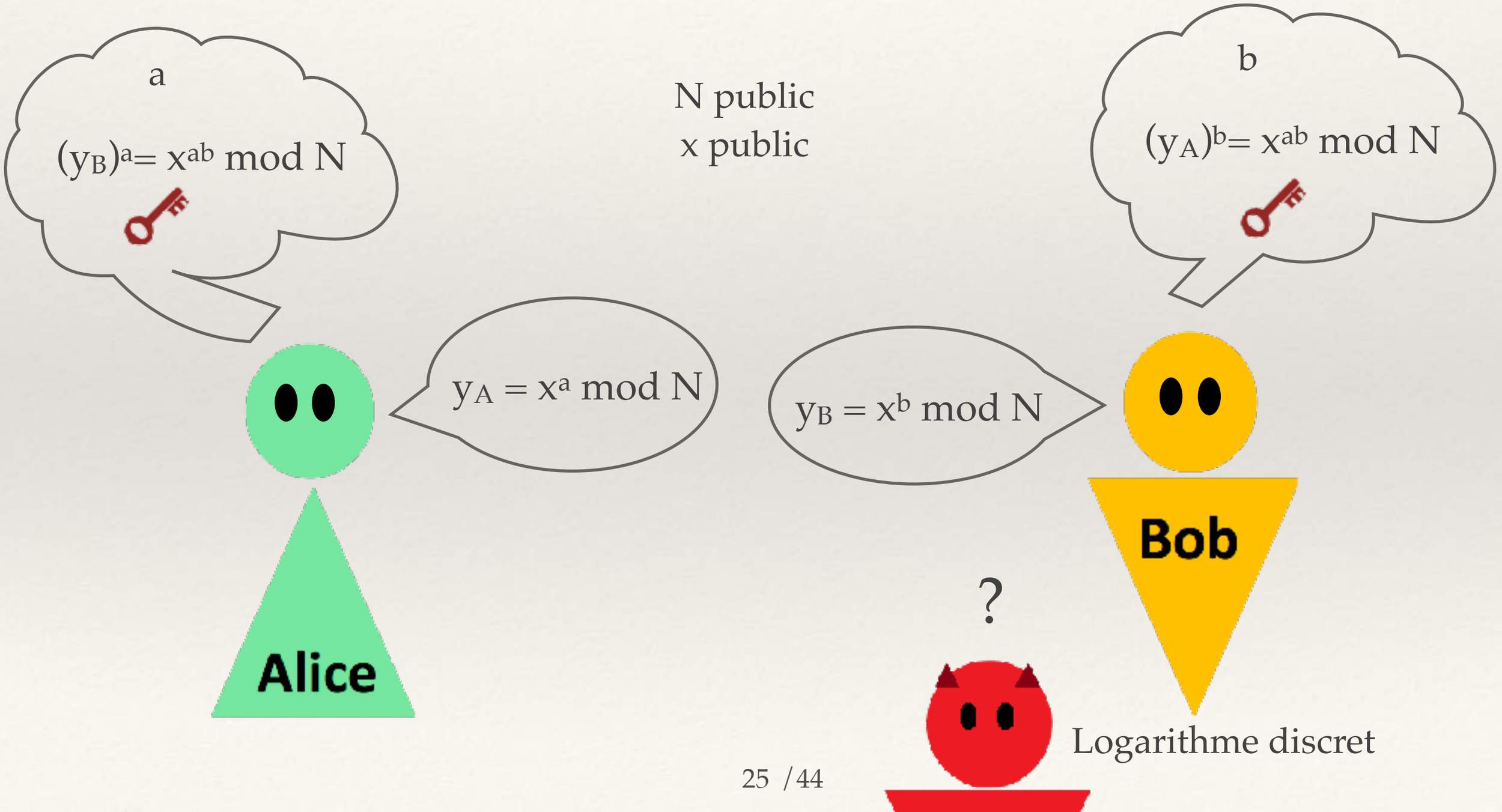
Ce logarithme est difficile à trouver

Diffie Hellman (années 80)

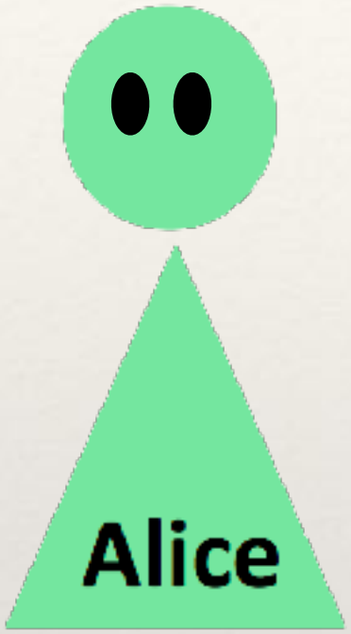
$$3^2 \bmod 7 = 9 \bmod 7 = 2$$

$$\ln_3(2) = ?$$

Diffie Hellman

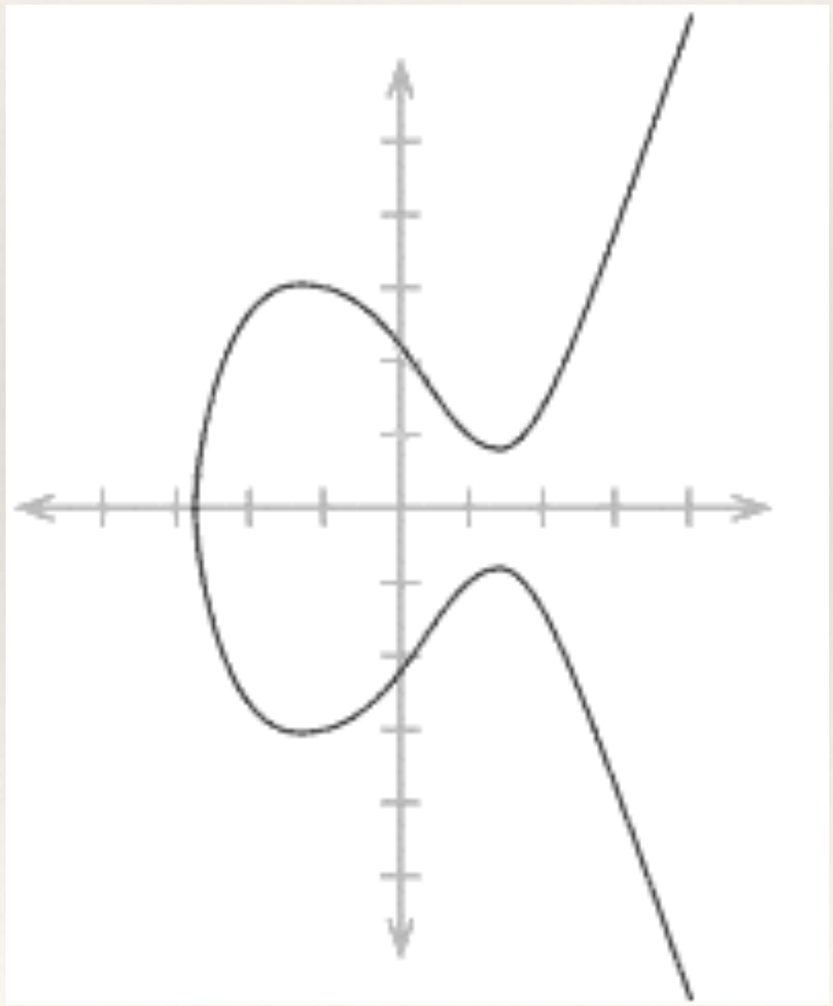


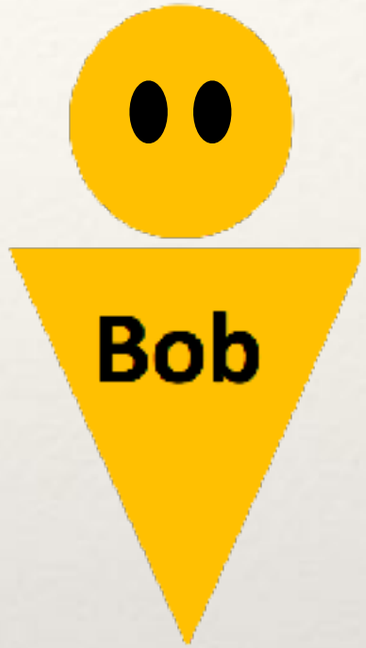
Cryptographie asymétrique



Sécurité basée sur la **factorisation** ou le **logarithme discret**

Différentes structures de groupes





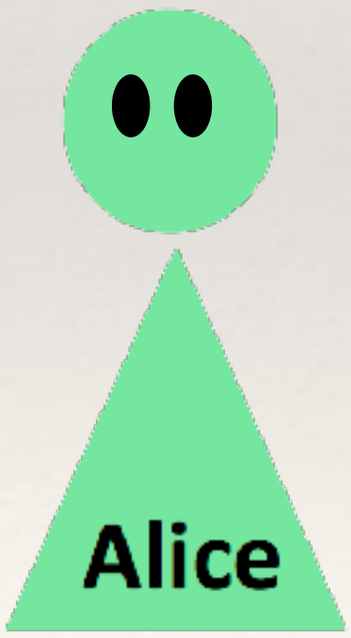
Confidentialité

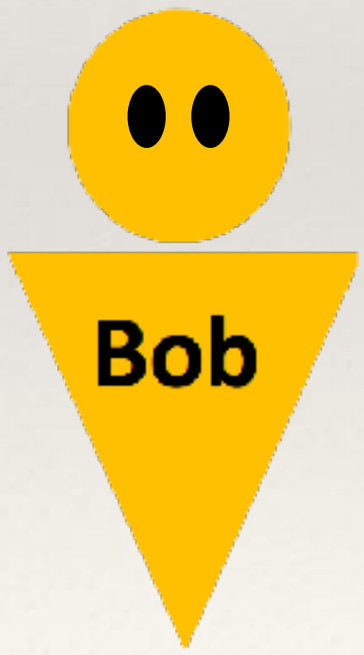
1) Etape de cryptographie asymétrique où définit une clé commune

Diffie Hellman **RSA**

2) Etape de cryptographie symétrique où échange des messages avec la clé commune

AES





Ce que permet la cryptographie

Confidentialité

Protection des communications et des données

- Militaires
- Médicales
- Bancaires
- Civiles
- IoT
- Cloud

Intégrité

Vérifier que les données n'ont pas été altérées

Authentification

Vérification d'identité, autorisations

Bitcoin

Cartes bleues

gemalto
security to be free

SAFRAN

oberthur
TECHNOLOGIES

De la crypto partout pour nous protéger

… Ou pour nous empêcher de frauder

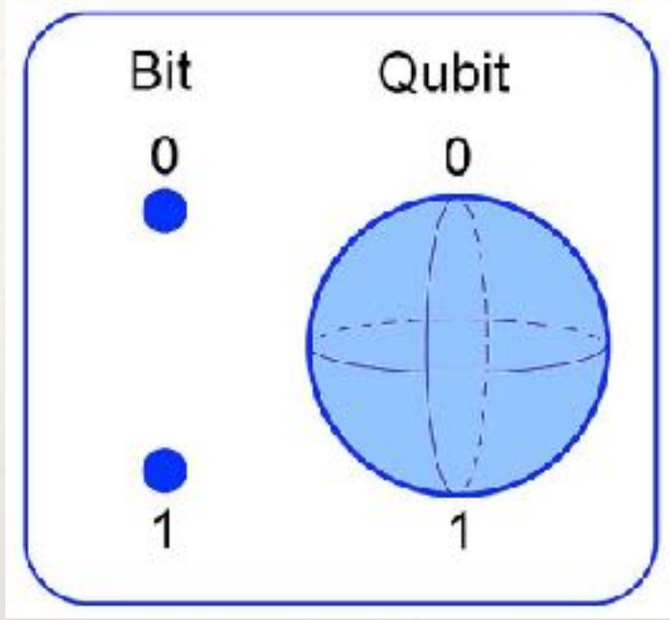
NETFLIX

CANAL+

Monde quantique

Bits : 0 ou 1

Quantum Bits : les deux en même temps



Algorithme quantique

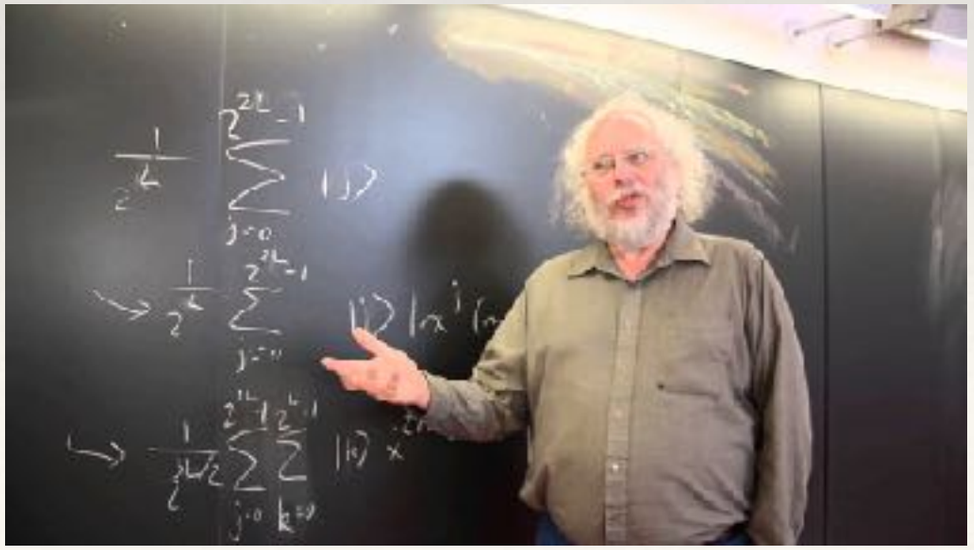
Circuits utilisant des Qubits pour effectuer des fonctions

Possibilité d'utiliser plusieurs Qubits en même temps

<u>Algorithme pour la factorisation et le logarithme discret</u>

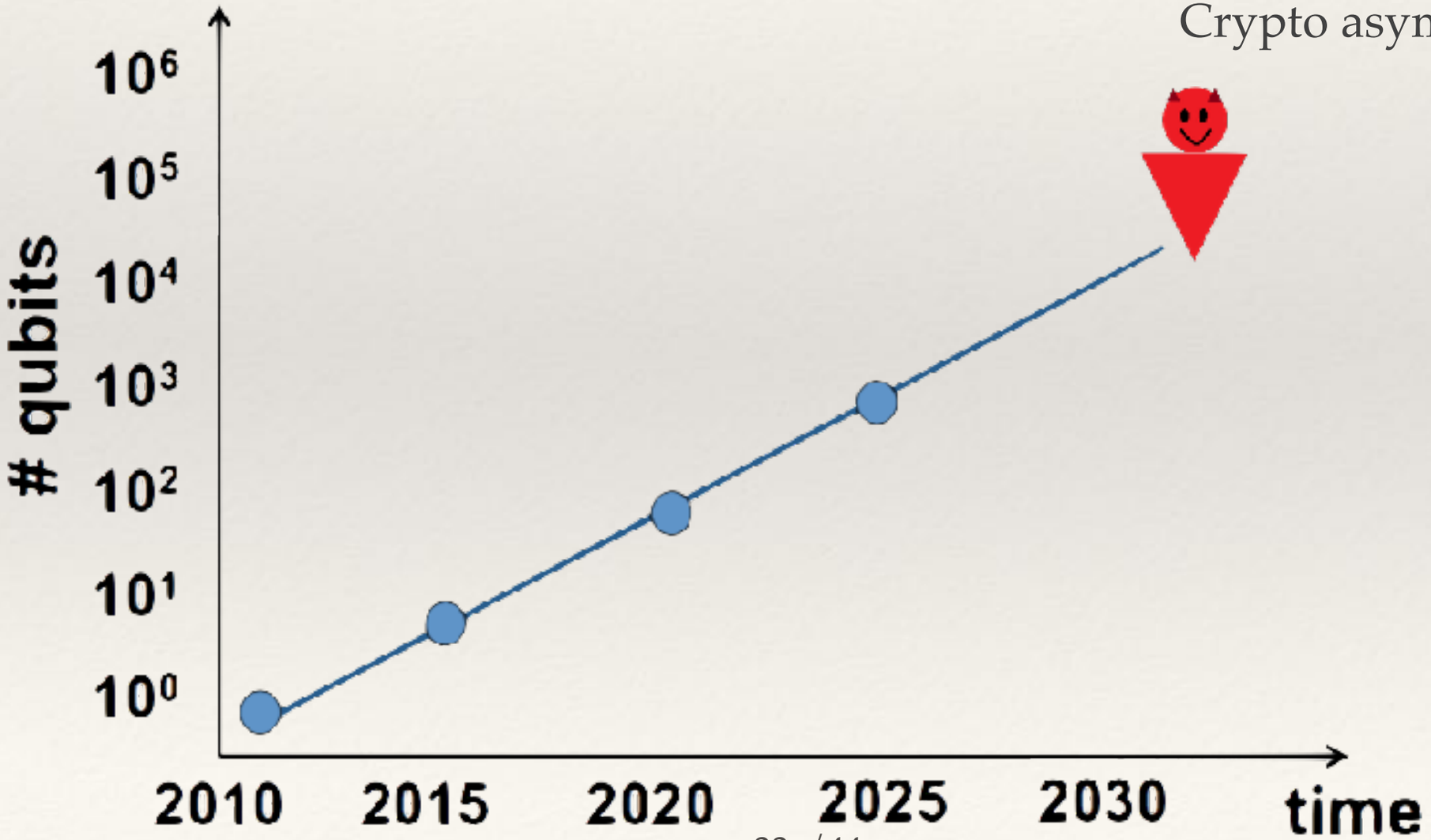
Années 2000

Peter Shor



Ordinateur quantique

On a l'algorithme mais on n'a pas encore l'ordinateur



La menace quantique

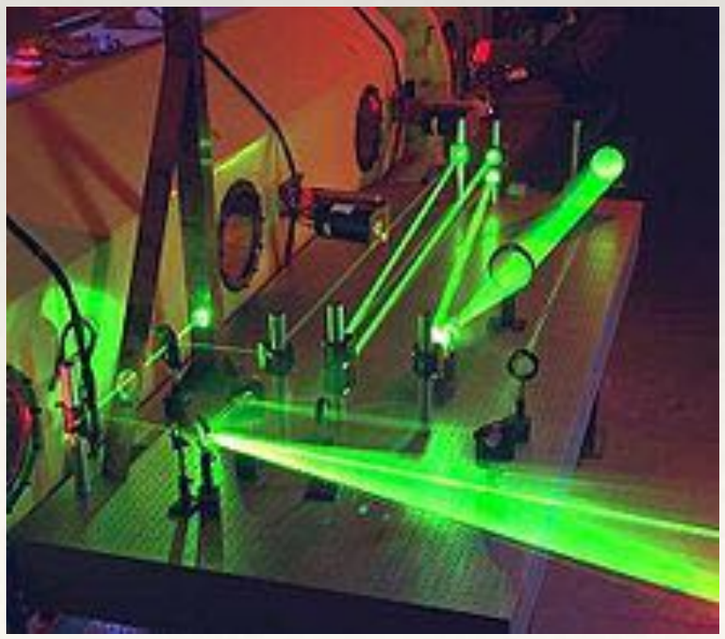
NSA : conseille vivement trouver des solutions

Semblent se rapprocher

Solutions possibles

Cryptographie quantique

Transmettre des Qubits intriqués
Nouvelles infrastructures réseau
Sécurité inconditionnelle



Cryptographie post-quantique

On garde les bits et les ordinateurs classiques
Nouveaux problèmes mathématiques plus difficiles
Autres que la factorisation et le logarithme discret

Compétition internationale

Commencée en 2017, fin prévue en 2020

National Institute of Standards and Technology
U.S. Department of Commerce

Une soixantaine de candidats
Beaucoup d'attaques en perspective
La France très bien représentée
Projet de recherche national

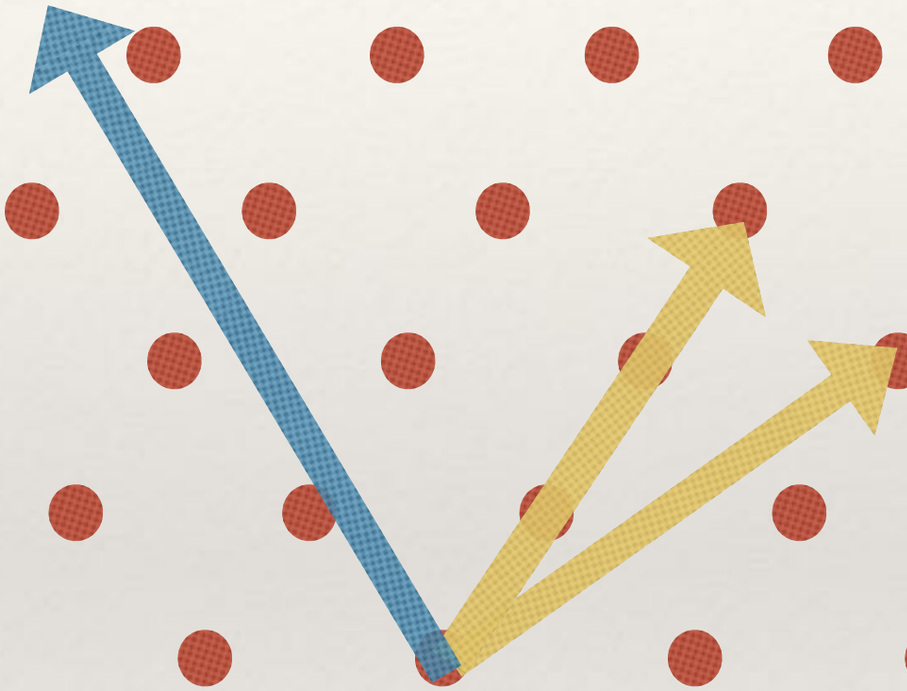
Les réseaux Euclidiens

Base

Shortest vector problem

A partir d'une base quelconque, trouver le vecteur le plus court.

CVP



Closest vector problem

A partir d’une base quelconque, trouver le vecteur du réseau le plus proche d’un vecteur donné

Finalement mon sujet, c'est

Utiliser des nouveaux problèmes mathématiques quantiques-résistants pour faire de la cryptographie

Cryptanalyse : attaques, analyses de sécurité de candidats

La recherche en crypto ?

Informatique très théorique :

- Etude de la difficulté algorithmique de certains problèmes mathématiques
- Classification des problèmes et leur difficulté relative

Informatique théorique :

- Définitions des différents types de sécurité
- Preuves de sécurité

Cryptographie

- Conception d'algorithmes basés sur des problèmes mathématiques
- Adapter les modèles aux problèmes actuels (Cloud, Blockchain, IA)

Cryptographie quantique

- Définir de la cryptographie utilisant des QuBits

La recherche en crypto ?

Cryptanalyse

- Définition de modèles d'attaques
- Attaques / Etude de la sécurité des algorithmes

Cryptanalyse par canaux auxiliaires

- Considérer les paramètres physiques des puces qui utilisent de la cryptographie
- Attaques utilisant la température, le temps, les rayonnement électromagnétique

Cryptanalyse quantique

- Attaquer en utilisant de la puissance quantique

Métiers dans la cryptologie

Chercheur en université

Quelles sont les formations ?

Universités

Licence Mathématiques /
Math info /
Math appliquées.

Certaines licences proposent des cours d'intro (Paris)

Ecoles d'ingénieurs

Mathématiques, informatique

Master de cryptologie (Paris, Limoges, Rennes, Bordeaux, Grenoble)

Doctorat de cryptologie

Des questions ?