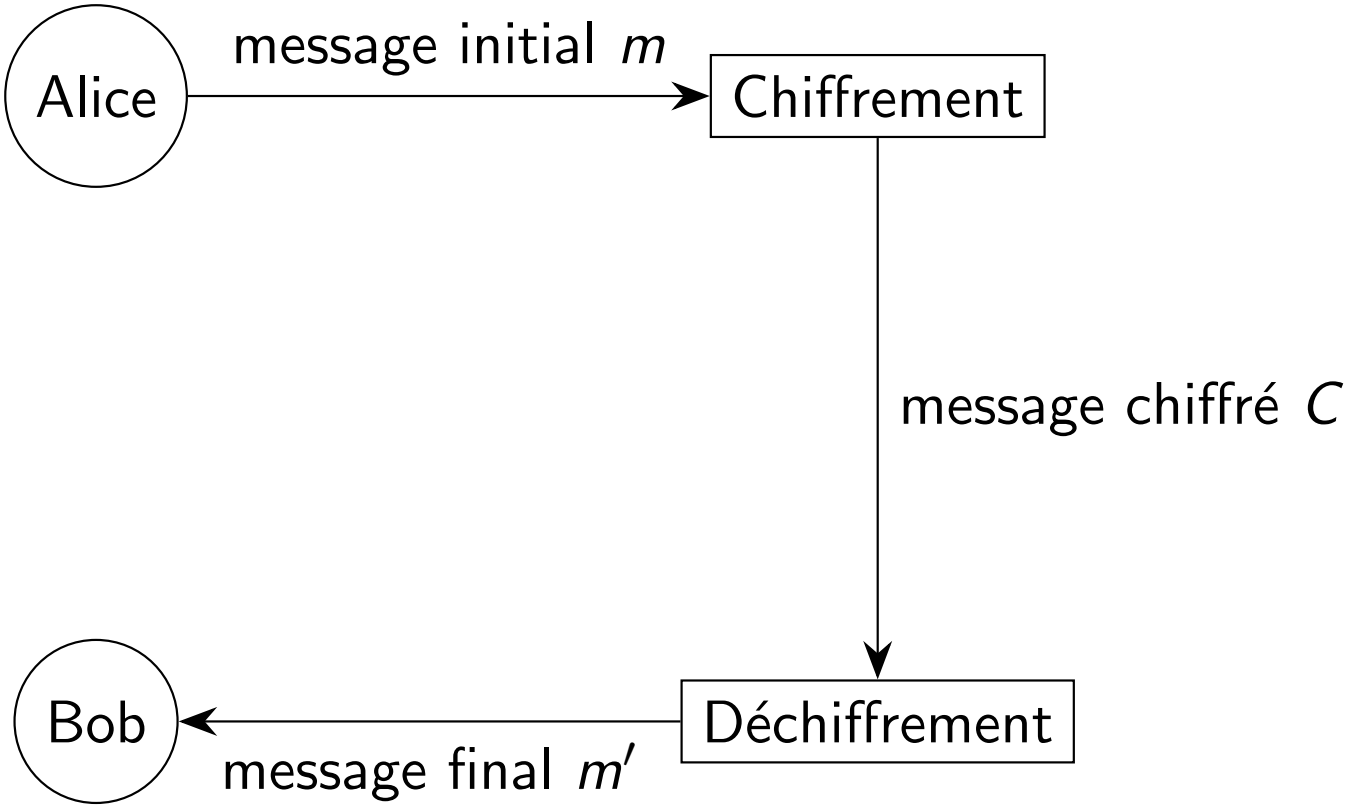
Cours d'introduction à la cryptographie

Vanessa VITSE

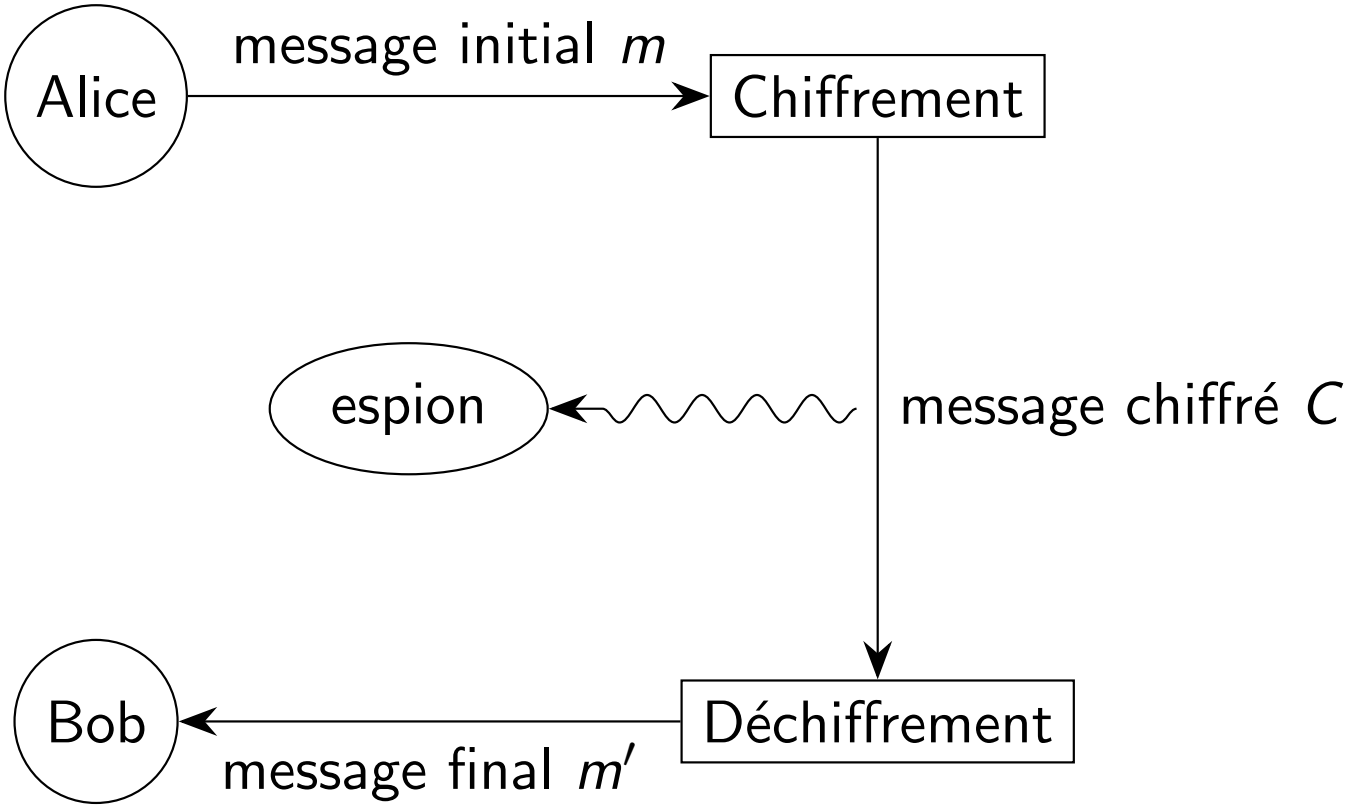
Université Grenoble Alpes

7 septembre 2020

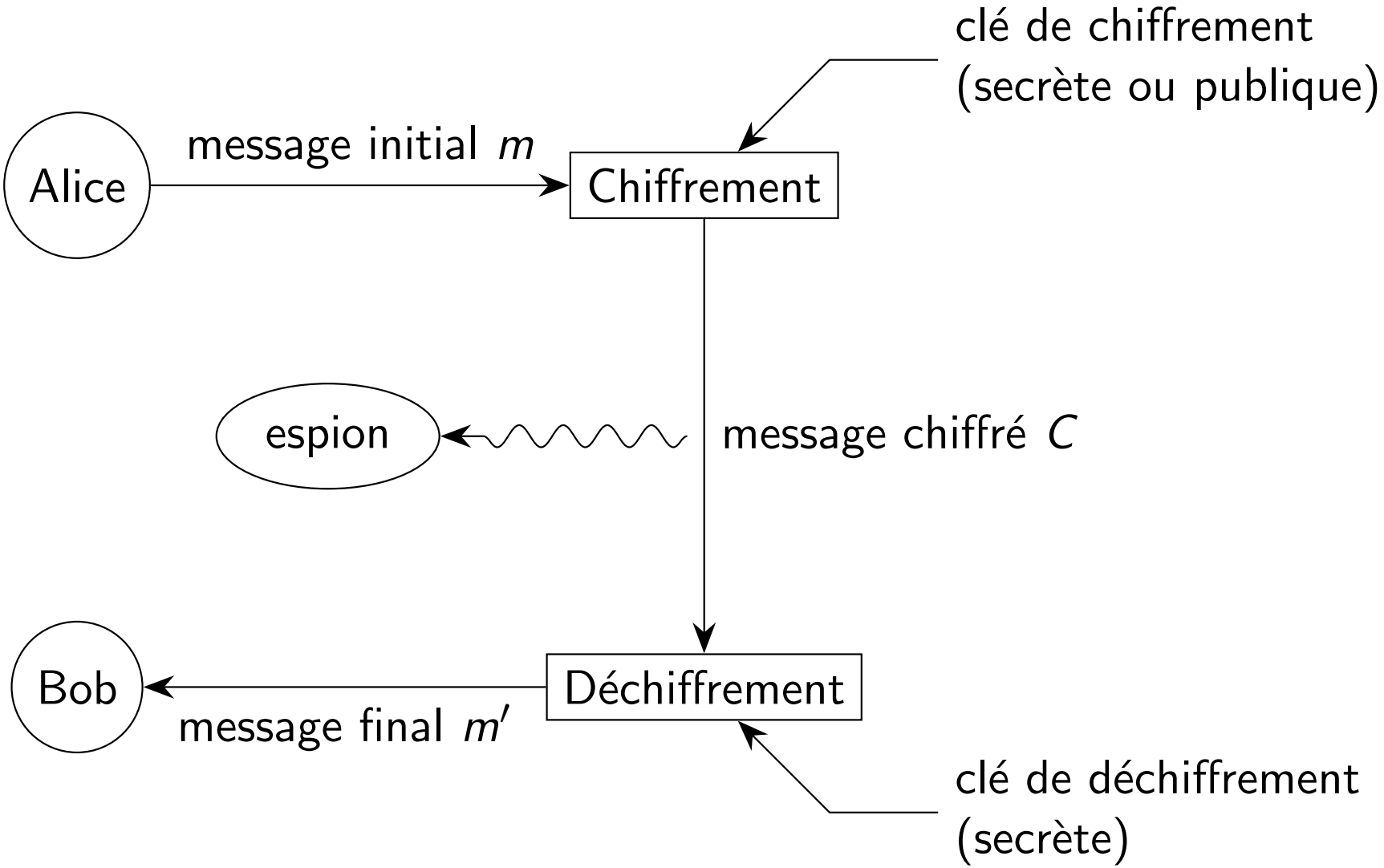
Introduction : cryptographie



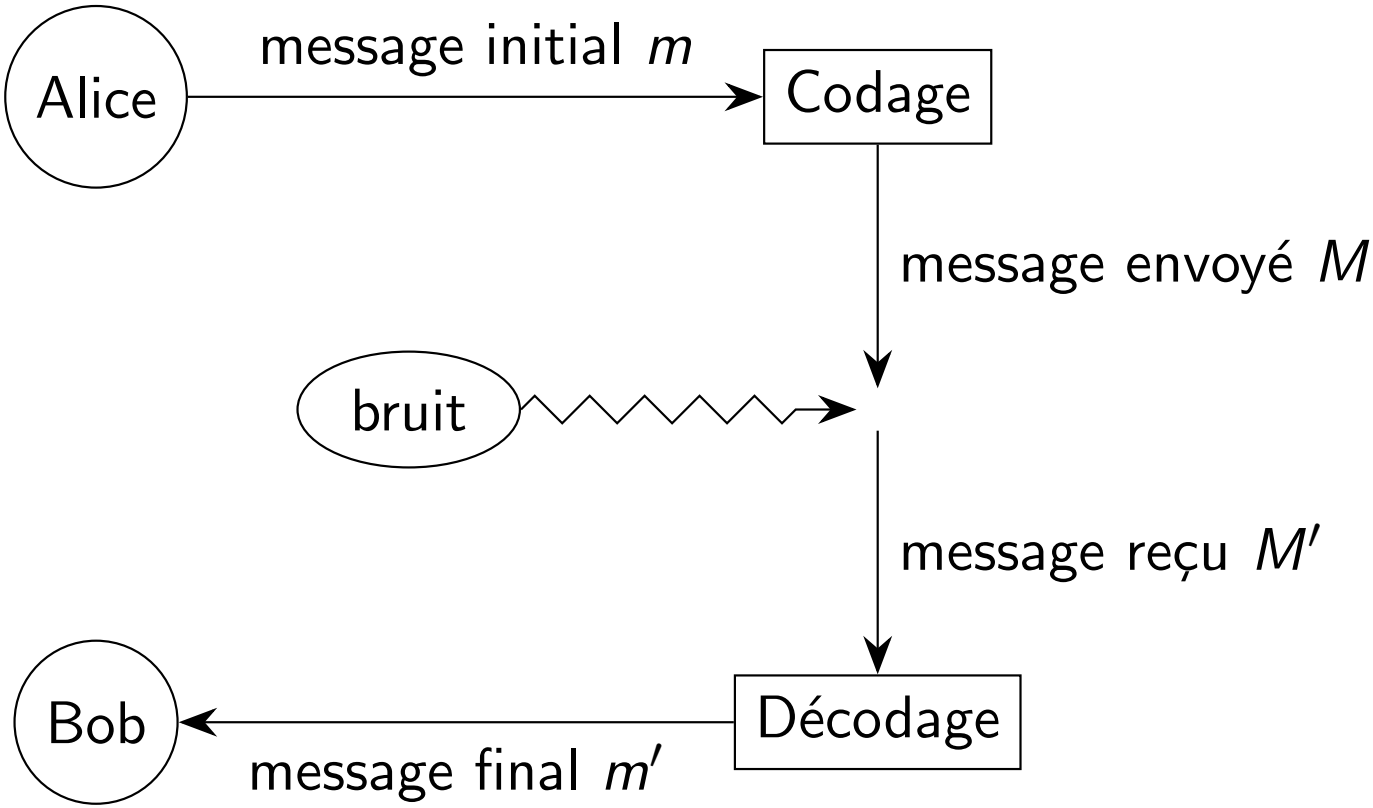
Introduction : cryptographie



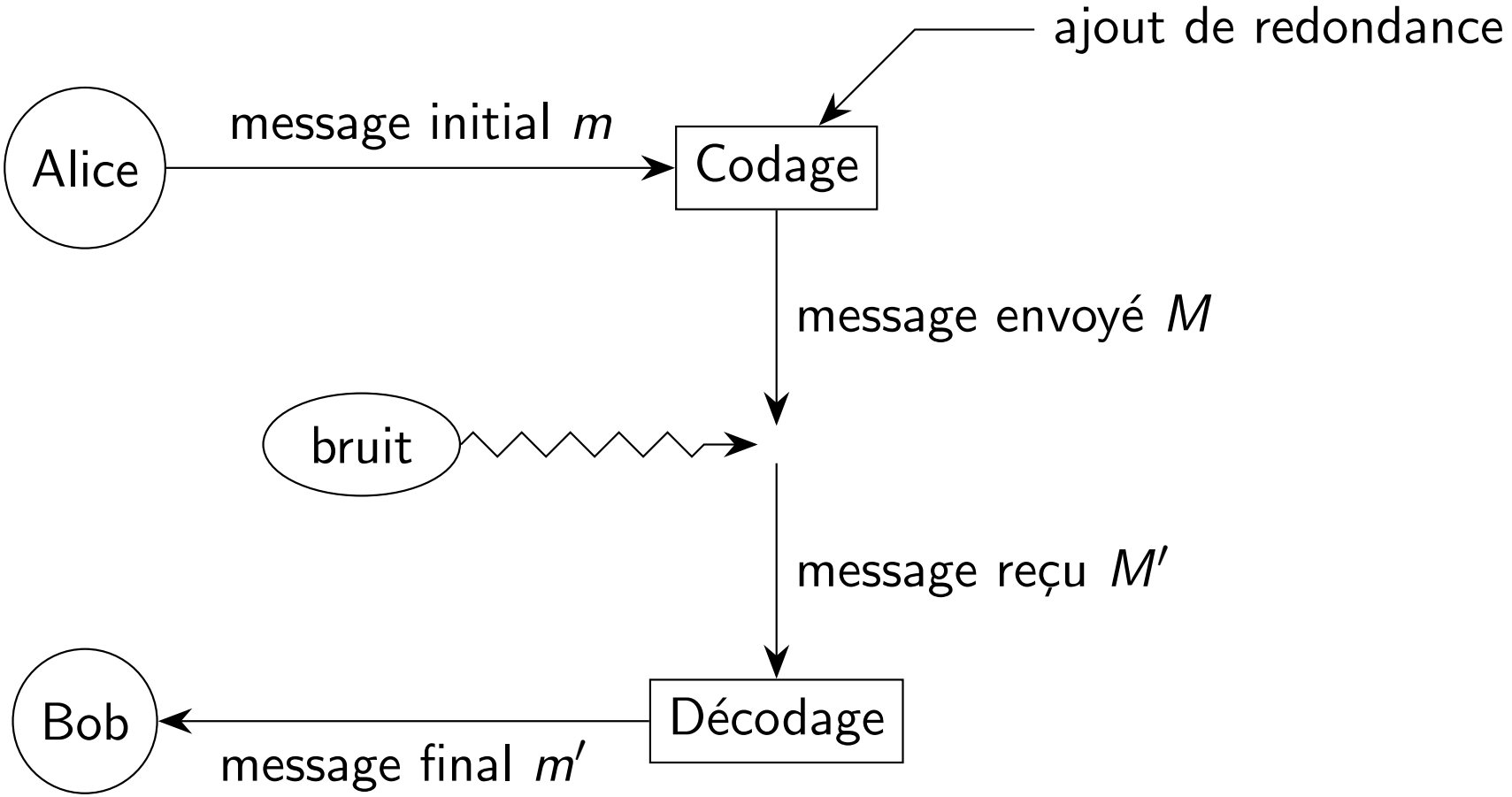
Introduction : cryptographie



Introduction : codes correcteurs



Introduction : codes correcteurs



Fondations mathématiques

Bases cryptographie / codage : arithmétique et algèbre (+ probas)

Besoin de savoir répondre aux questions suivantes (entre autres !)

- Arithmétique modulaire : calculs pratiques modulo un entier/polynôme ?
  Construction/manipulation des corps finis (surtout non premiers) ?
- Nombres premiers : comment les trouver ? les certifier ?
  Comment factoriser ?
  Même questions avec les polynômes irréductibles.
- Peut-on produire algorithmiquement des nombres aléatoires ?

Applications

Exemples d'**applications concrètes** de mathématiques fondamentales :

- Protocoles classiques de cryptographie à clef publique
  - basés sur la factorisation : RSA en chiffrement et en signature
  - basés sur les logarithmes discrets : échange de clefs de Diffie-Hellman, chiffrement d'ElGamal
- Constructions de codes correcteurs d'erreurs : codes cycliques et polynomiaux
- Générateurs pseudo-aléatoires basés sur les récurrences linéaires

Modalités

- 8 séances de CM + TD/TP sur machines
  a priori en SageMath, prévoir installation sur machine personnelle
- évaluation : CC sur machine + examen terminal écrit

Modalités

- 8 séances de CM + TD/TP sur machines
  a priori en SageMath, prévoir installation sur machine personnelle
- évaluation : CC sur machine + examen terminal écrit

UE importante pour :

- agrégation, particulièrement option C (calcul formel)
- poursuite d'études M2 Cybersécurité ou M2 CSI (alternance)