Algèbre effective et cryptographie

Bernard Parisse – Vanessa Vitse

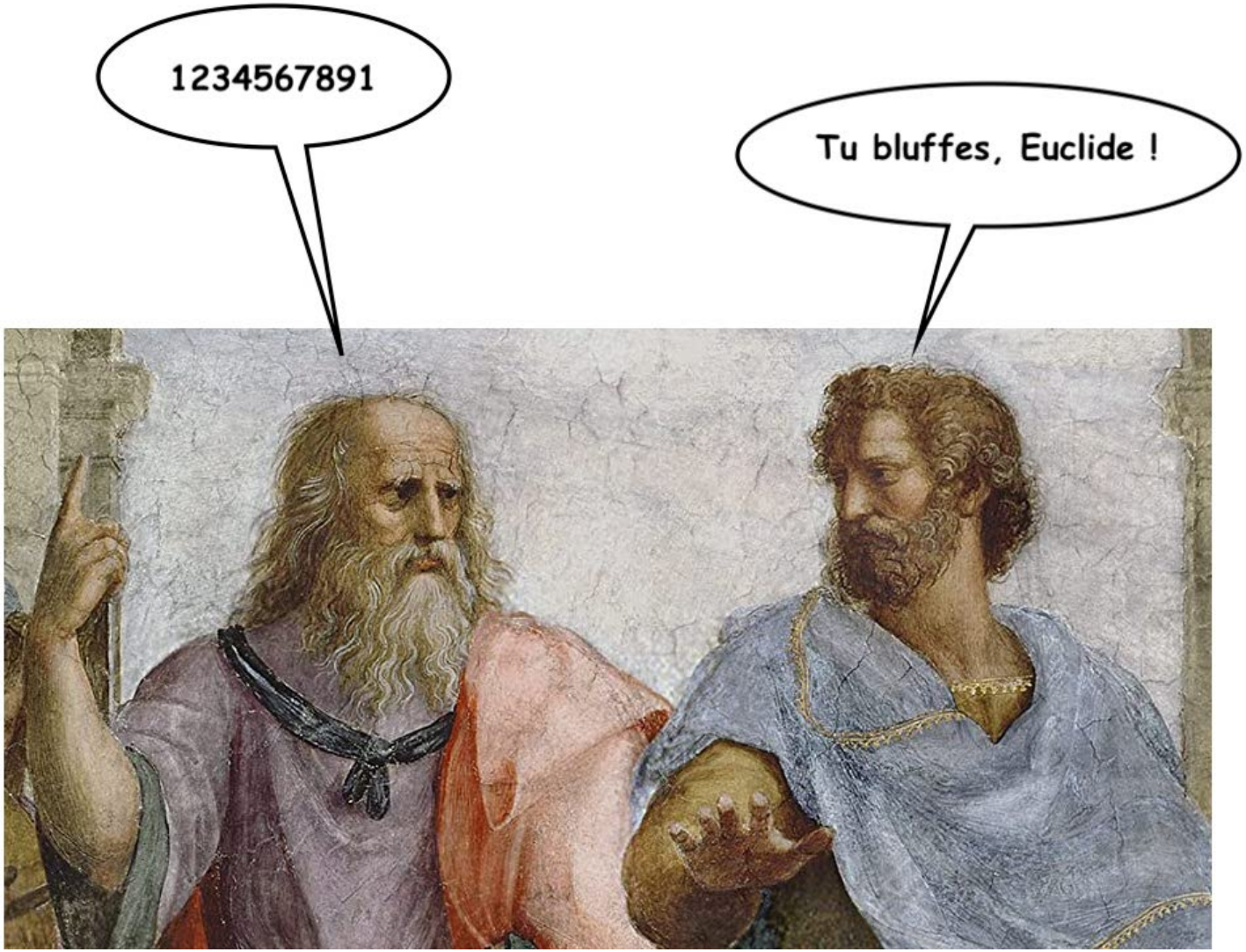
Université Grenoble Alpes

6 septembre 2021

Algèbre effective, quésaco ?

Algèbre effective, quésaco ?

Algèbre effective, quésaco ?



« Il existe une infinité de nombres premiers »

- La preuve d'Euclide est-elle constructive ?

« Il existe une infinité de nombres premiers »

- La preuve d'Euclide est-elle constructive ? (Non)

« Il existe une infinité de nombres premiers »

- La preuve d'Euclide est-elle constructive ? (Non)
- Est-ce que vous connaissez une méthode pour construire des (grands) nombres premiers ?

« Il existe une infinité de nombres premiers »

- La preuve d'Euclide est-elle constructive ? (Non)
- Est-ce que vous connaissez une méthode pour construire des (grands) nombres premiers ?
- Cette méthode est-elle efficace ?

Philosophie générale

Étant donnée une structure algébrique

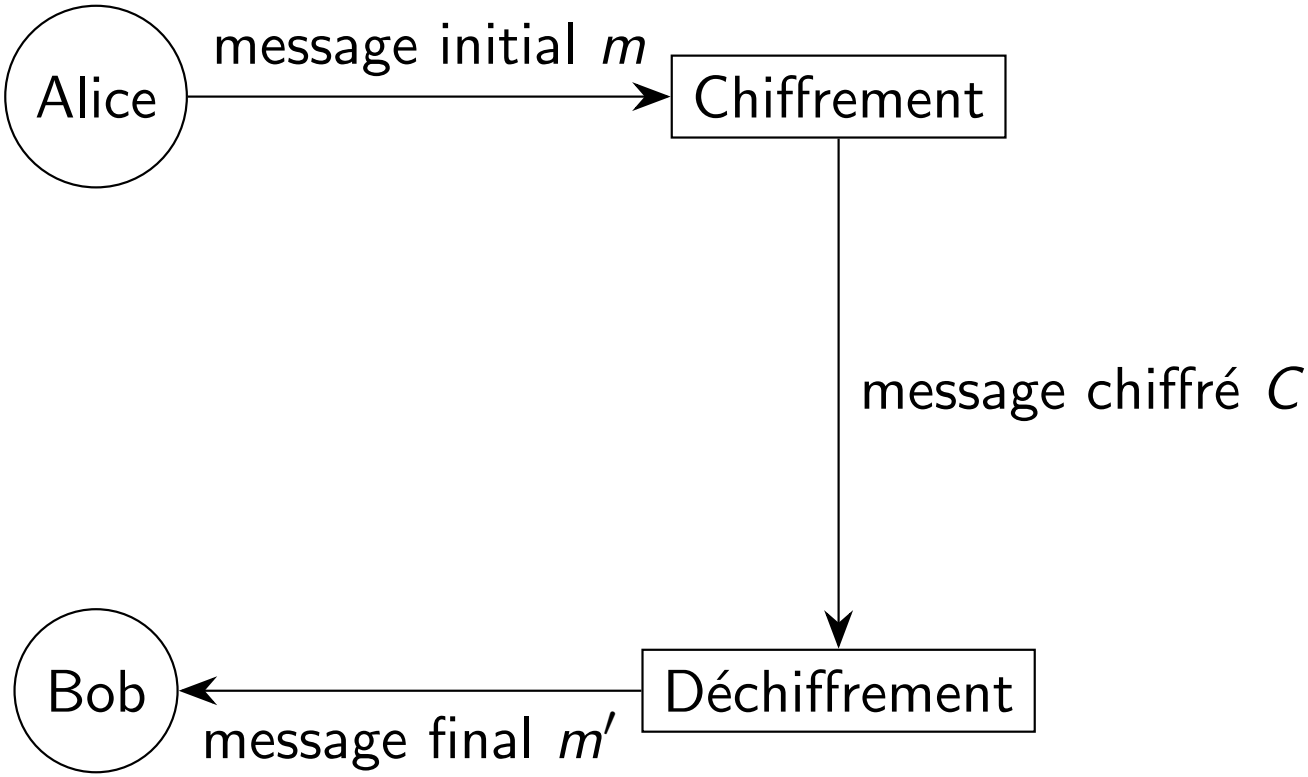
- peut-on représenter ses éléments en machine ?
- peut-on calculer efficacement avec ?
- pour tout théorème d'existence, a-t-on un algorithme pour constuire l'élément ? cet algorithme est-il efficace ?

Philosophie générale

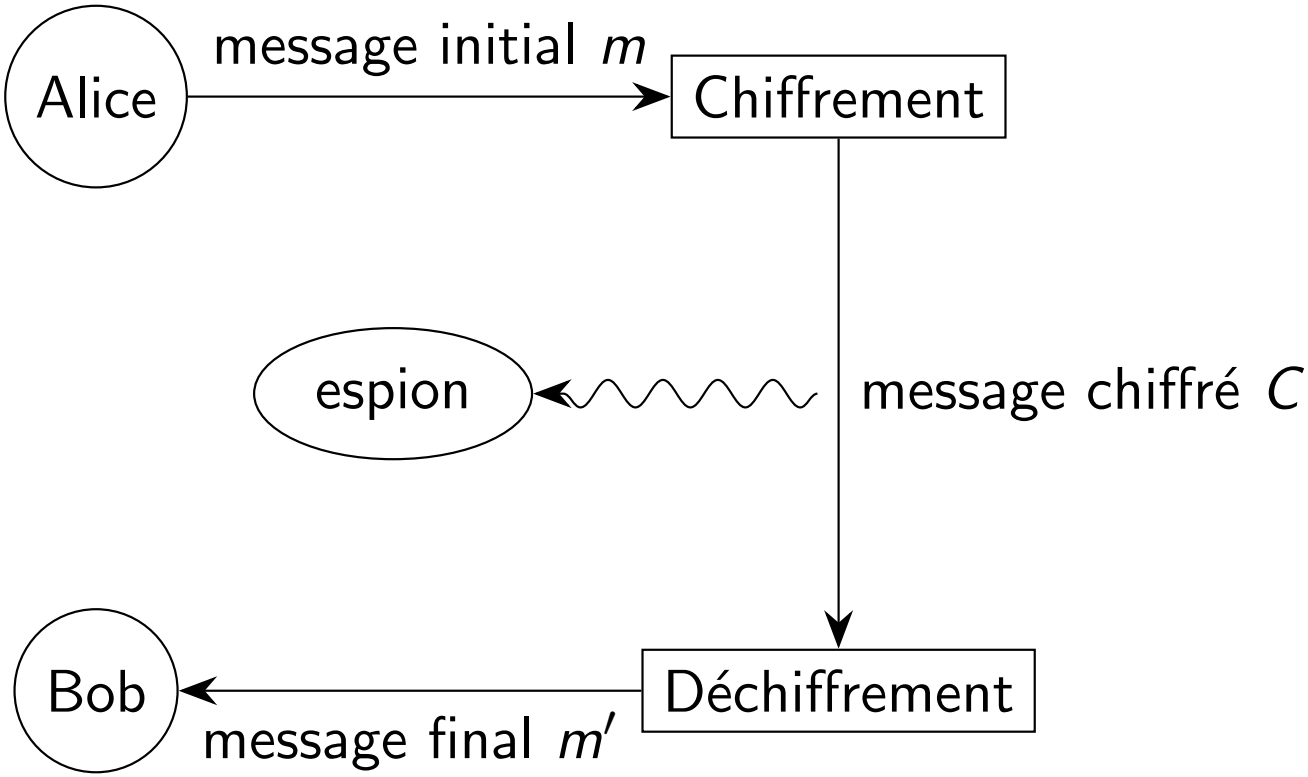
Étant donnée une structure algébrique

- peut-on représenter ses éléments en machine ?
- peut-on calculer efficacement avec ?
- pour tout théorème d'existence, a-t-on un algorithme pour constuire l'élément ? cet algorithme est-il efficace ?
- **qu'est-ce qu'on peut faire avec tout ça dans la vraie vie ?**

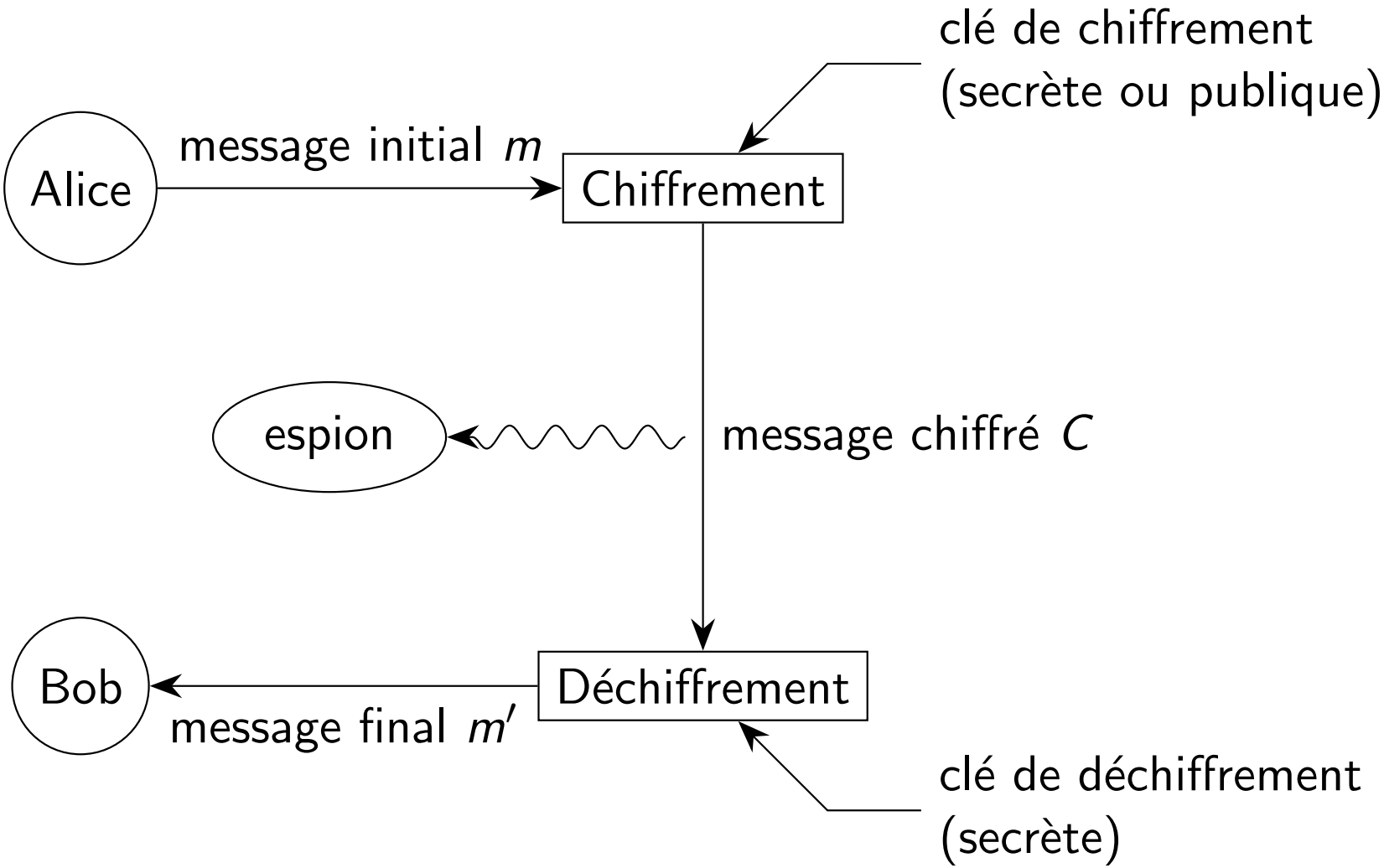
Une application : la cryptographie



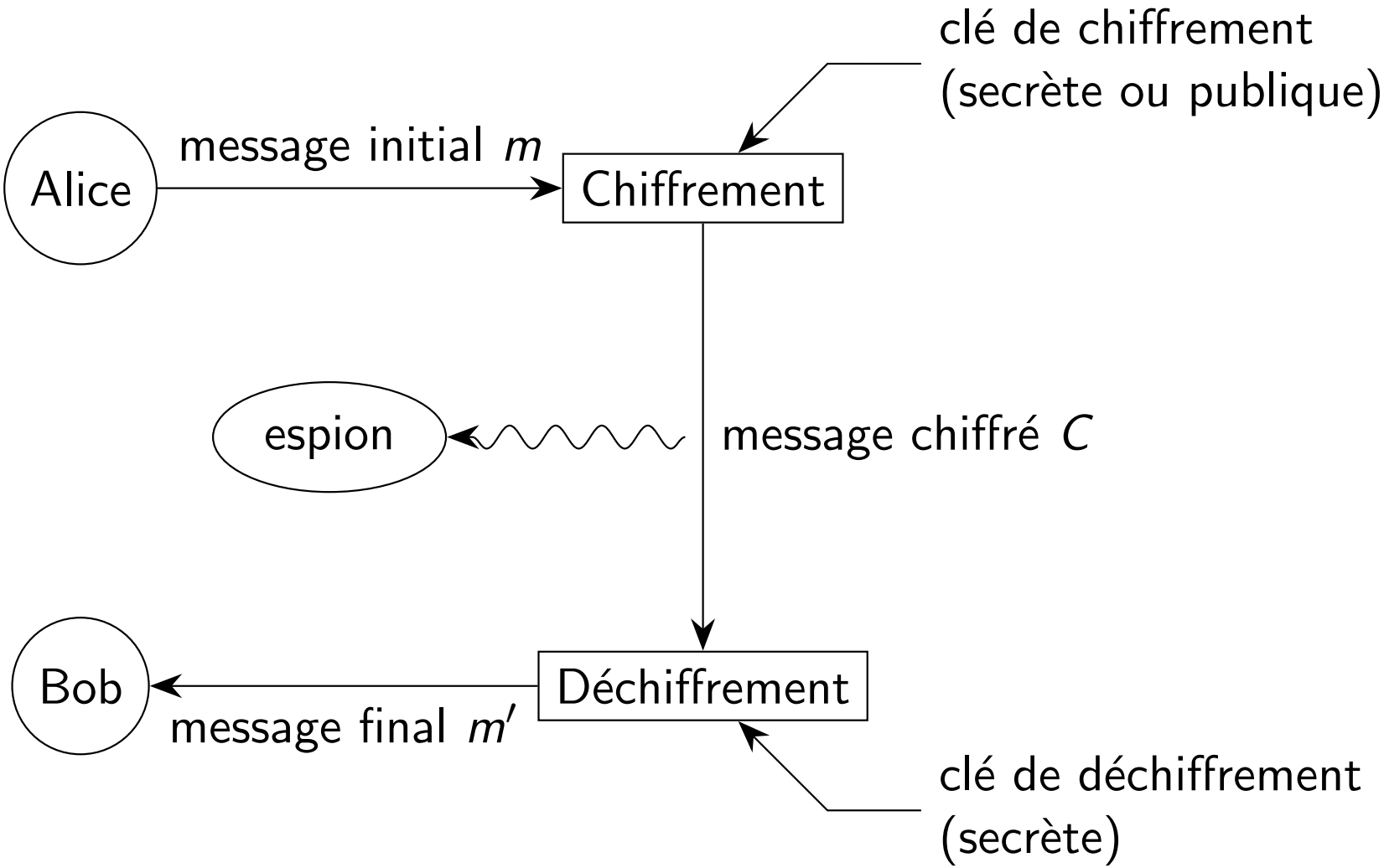
Une application : la cryptographie



Une application : la cryptographie



Une application : la cryptographie



Utilise arithmétique et algèbre (+ probas)

Contenu de l'UE

- 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.
  Idem avec les polynômes irréductibles.

- Protocoles classiques de cryptographie à clef publique
  - basés sur la factorisation : RSA
  - basés sur les logarithmes discrets : Diffie-Hellman

- Constructions de codes correcteurs d'erreurs

- ...

Modalités

- 21h de CM
- 33h réparties entre TD et TP sur machines, logiciel Xcas
- évaluation :
  - préparation d'un mini-projet sur un thème au choix et présentation orale
  - examen écrit

Modalités

- 21h de CM
- 33h réparties entre TD et TP sur machines, logiciel Xcas
- évaluation :
  - préparation d'un mini-projet sur un thème au choix et présentation orale
  - examen écrit

UE importante pour :

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