

# Rapport MT10 - TP2 : Autour du RSA

Martin Schneider, Océane Bordeaux

10 mai 2022

# Contents

<b>1</b>	<b>Préliminaire : SageMath et les nombres entiers</b>	<b>2</b>
<b>2</b>	<b>Nombres premiers</b>	<b>2</b>
2.1	Sur la répartition des nombres premiers . . . . .	2
2.2	Nombres de Fermat . . . . .	2
2.3	Nombres de Mersenne . . . . .	2
2.4	Un test de primalité pour les nombres de Mersenne . . . . .	2
<b>3</b>	<b>Algorithmes d'exponentiation</b>	<b>2</b>
3.1	Naïf itératif et naïf récursif . . . . .	2
3.2	Dichotomique itératif et dichotomique récursif . . . . .	2
3.3	Algorithme d'exponentiation modulaire . . . . .	2

- 1 Préliminaire : SageMath et les nombres entiers
- 2 Nombres premiers
  - 2.1 Sur la répartition des nombres premiers
  - 2.2 Nombres de Fermat
  - 2.3 Nombres de Mersenne
  - 2.4 Un test de primalité pour les nombres de Mersenne
- 3 Algorithmes d'exponentiation
  - 3.1 Naïf itératif et naïf récursif
  - 3.2 Dichotomique itératif et dichotomique récursif
  - 3.3 Algorithme d'exponentiation modulaire