# **Rapport Projet Cryptographie**

## Jarvis:Users:Jarvis:Documents:UCP:M1:Crypto:Projet:Crypto:Crypto:doc:Graph-sieve.pdfTest de primalité

Trois implémentations différentes pour tester si P est polynôme premier dans F\_2[X] :

1. Parcours de tous les polynômes D de degré inférieur à P. Si le reste de la division euclidienne de chaque division est nul, alors P est premier
2. Même test, mais parcours uniquement à partir de C, avec C.C = P
3. Méthode du crible d’Eratosthène : Chaque polynôme est multiplié avec ses polynômes de degré moindre, et le polynôme résultat est noté comme non premier. Lorsque les itérations dépassent P, on a obtenu la liste des polynômes premiers jusqu’à P. Reste à vérifier que P appartient bien à la liste

## Test de primitivité

1. Vérification que P est premier
2. Vérification que X est générateur pour F\_2[X]/P
   1. Si l = deg(P), on cherche les diviseurs di de 2^l-1
   2. Si le résultat de toutes les divisions euclidiennes de P par X^di est égal à 1, alors P est bien primitif