——————————————————————————————————————————

**Protocole d’interrogation anonyme de base de données**

——————————————————————————————————————————

# Sommaire :

[Sommaire : 3](#_Toc1)

[Introduction 4](#_Toc2)

[Chiffrement de Paillier 5](#_Toc3)

[Protocole d’échange anonyme 6](#_Toc4)

[Approfondissement 7](#_Toc5)

[Conclusion 8](#_Toc6)

Introduction

Chiffrement de Paillier

Voici le protocole d'implémentation :

1. Génération des clés
   1. Choisir deux nombres premiers p et q de taille égale
   2. Calculer n = p \* q et lambda = ppcm(p-1, q-1)
   3. On fixe g = n+1 // est random à la base
   4. Calculer mu = lambda^-1 mod n

La clé publique est (n, g), la clé privée est (lambda, mu)

1. Chiffrement
   1. Soit m un message à chiffrer, m ∈ Zn
   2. Choisir un nombre aléatoire r ∈ Zn\*
   3. Calculer le chiffré c = (g \* m) \* rn mod n2 // c'est gm à la base
2. Déchiffrement
   1. Soit c le chiffré à déchiffrer
   2. Calculer le déchiffré m = (clambda mod n2 - 1) / n \* mu mod n

Protocole d’échange anonyme

Approfondissement

Conclusion