Pour ajouter une partie de cryptanalyse RSA, nous devons implémenter un algorithme qui trouve la clé privée et le message en clair à partir des informations publiques. L'un des moyens classiques pour cela est d'utiliser une attaque par factorisation des clés publiques pour retrouver les clés privées.

Pour simplifier cette démonstration, nous allons implémenter une méthode brute-force de factorisation de n en ses composants premiers p et q. À partir de là, nous pouvons calculer la clé privée d et déchiffrer un message.

Ces ajouts permettront de factoriser n, de calculer d, puis de déchiffrer le message chiffré en utilisant la cryptanalyse RSA.