Table des matières

[INTRODUCTION 2](#_Toc86010944)

[I. CONTEXTE DU PROJET 3](#_Toc86010945)

[1. Définition et pertinence d’un réseau communautaire 3](#_Toc86010946)

# INTRODUCTION

De nos jours, internet est devenu un moyen essentiel de communication, d’accès aux services et à l’information. Pourtant, un pan entier de l’humanité est encore privé d’un moyen d’accès abordable et fiable au réseau mondial. Face au défi que représente la résorption des inégalités numériques, l’amélioration de la couverture des services mobiles à large bande n’est pas nécessairement la solution, car elle relève des moyens techniques d’entreprises privées de télécommunication, elle est coûteuse pour la collectivité et elle n’est pas nécessairement abordable pour les usagers. C’est pourquoi se sont développées des initiatives locales et autogérées : les réseaux communautaires. Ceux-ci s’appuient sur des infrastructures informatiques légères et modulaires qui permettent à chacune d’acquérir les compétences et les outils nécessaires pour le maintien et l’enrichissement de leurs contenus. Toutefois, chaque réseau possède sa propre politique de cryptage des échanges (messages, appels, Visio, etc…). Ainsi, il est nécessaire de mettre en place des systèmes cryptographiques performants sur ces réseaux. De ce fait, il sera question pour nous d’étudier le protocole de cryptographie signal. Ceci passera par une présentation du contexte, suivi d’une présentation du projet, puis d’une exposition des méthodes utilisées appuyée par une implémentation.

# CONTEXTE DU PROJET

## Définition et pertinence d’un réseau communautaire

Les réseaux communautaires sont des infrastructures de télécommunications déployées et exploitées par un groupe local pour répondre à ses propres besoins de communication. Ils sont le résultat de personnes travaillant ensemble, combinant leurs ressources, unissant leurs efforts et se rapprochant pour combler les lacunes de connectivité dans une zone donnée.