

Résumé. Dans ce travail, nous tentons d'explorer la contribution pour la cryptanalyse des chiffres simples d'une méta-heuristique récente et souvent méconnue : la '*Recherche Dispersée*' (*Scatter Search*). Nous essayons d'illustrer la faisabilité de son utilisation en tant qu'outil de cryptanalyse. Cette méta-heuristique évolutive basée population, est basée sur une approche pour la programmation discrète développé par Fred GLOVER. Elle utilise des combinaisons linéaires de parties de la population pour créer de nouvelles solutions.

Nous avons implémenter les méthodes de la recherche dispersée pour la cryptanalyse des chiffres simples ; ensuite, nous avons effectué des expérimentation pour fixer les paramètres des procédures, et pour évaluer les performances de la méthode ; enfin, nous avons dressé une comparaison avec un algorithme génétique.

Mots-clé. Cryptanalyse. Chiffres simples. Substitution. Transposition. Recherche Dispersée. Recherche heuristique. Approche évolutive. Problème d'optimisation.

Abstract. In This work, we tempt to explore the contribution of a recent meta-heuristic –the *Scatter Search*– for the cryptanalysis of simple ciphers. We try to illustrate the feasibility of its use as a cryptanalysis tool. This evolutionary meta-heuristic is based on an approach for the discreet programming developed by Fred GLOVER. It use linear combinations of population's subsets in order to generate new ones.

We've implemented scatter search's methods for the cryptanalysis of simple ciphers; then, we did the experimentation to fix parameters of the procedures, and to evaluate the method's performances. finally, we raised a comparison with a genetic algorithm.

Keywords. Cryptanalysis. Simple ciphers. Substitution. Transposition. Scatter Search. Meta-heuristic. Evolutionary Algorithm. Optimisation problems.