Лабораторная работа 1

ФИО

Михайлов Даниил Дмитриевич (6111-100503D)
Мальгин Дмитрий Станиславович (6111-100503D)

Topic

Privacy Preserving Data Mining; Secure Multi-Party Computation; Homomorphic Encryption

Описание предметной области

Privacy Preserving Data Mining — это методология, которая позволяет анализировать данные, не раскрывая конфиденциальную информацию. Secure Multi-Party Computation — это подход, позволяющий нескольким участникам выполнять вычисления над своими данными, не раскрывая их друг другу. Homomorphic Encryption - это метод шифрования, который позволяет выполнять операции над зашифрованными данными без их расшифровки. Эти методы в совокупности обеспечивают защиту конфиденциальности данных при их анализе и обработке. В сфере информационной безопасности эти технологии играют ключевую роль в защите информации.

Недостаток (Gap)

В статье не объясняется почему алгоритмы интеллектуального анализа данных сложны. Так же в статьях отсутствует информация о стойкости шифрования. И не описывается в чем сложность создания полного гомоморфного шифрования. Непонятно, возможно ли объединить несколько алгоритмов в один.

Идея

Совместить данные типы шифрование в один и узнать его устойчивость.

Краткий текст обзора

якпвввввврявекккккккккккккккккккккккккккккккквякрвякряукряук