Доброго дня, шановні пані та панове.

Мета мого дослідження – підвищення ефективності шифрування повідомлень великого розміру в хмарних сховищах даних.

Об'єкт мого дослідження - процес швидкого шифрування даних великого розміру.

Предмет мого дослідження - математичні моделі та методи швидкого шифрування повідомлень великого розміру.

Розроблений алгоритм взяв ідеї блочних і табличних шифрів та поєднав їх.

І це працює розроблений шифр наступним чином:

Спочатку, алгоритм ділить відкритий текст на блоки довжиною ключа. Потім, на першому раунді перший блок шифрується алгоритмом Віженера, та використовує ключ, як вектор ініціалізації, інші блоки використовують минулий шифроблок, як вектор ініціалізації, щоб здомогтися лавинного ефекту. На наступних раундах перший блок використовує останній шифроблок, як вектор ініціалізації. Така конструкція дозволяє керувати часом і безпекою шифру. Тобто, при збільшенні кількості раундів, шифр працює надійніше, але потребує більше часу, і навпаки. Дослідження та криптоаналіз написаного шифру показав, що розроблений алгоритм працює краще за інші в моєму списку з даними великого обсягу.

Було створено дві програми, де можна було б використовувати розроблений алгоритм. По-перше, це консольний чат, який можна запускати на будь-якому обладнанні та сайт-програму, яка шифрує файли на Google Drive, так що навіть компанія Google не матиме доступу до ваших даних.

Для зберігання файлів великого розміру на хмарних сховищах даних краще всього себе продемонстрував саме розроблений шифр, через можливість керування часом роботи алгоритму і його криптостійкістю. Даний алгоритм має більш надійну криптостійкість у порівнянні з шифром Віженера та шифром SAFER, не потребує генерації великої кількості випадкових чисел, як шифр Вєрнама, та працює набагато швидше за шифр DES.

Підводячи підсумок, моє дослідження показало, що для великих даних краще використовувати розроблений алгоритм, який може бути застосований в програмах подібних написаним.

Дякую за увагу.