Гомоморфное шифрование в защите информации

Актуальность

Данное исследование является актуальным, поскольку в настоящее время широкое развитие получили технологии облачных вычислений, при этом особое внимание уделяется конфиденциальности и безопасности информации.

Целью данного исследования является изучение различных подходов гомоморфного шифрование, а также разработка прикладного ПО, реализующего один из этих подходов, проверка гомоморфных свойств выбранного для реализации алгоритма шифрования.

Цель

Целью настоящего исследования является изучение различных подходов гомоморфного шифрование, а также разработка прикладного ПО, реализующего один из этих подходов, проверка гомоморфных свойств выбранного для реализации алгоритма шифрования.

Основы гомоморфного шифрования.

Гомоморфное шифрование

- Шифрование – это обратимое преобразование данных с целью сокрытия их от неавторизованных лиц.
- Гомоморфное шифрование (ГШ) – это технология, позволяющая производить вычисления над зашифрованными данными без необходимости их предварительного расшифровывания. Это открывает новые возможности для безопасной работы с данными. Благодаря использованию данной технологии, появляется возможность проведения обработки конфиденциальных данных, используя сторонние вычислительные ресурсы.

История развития гомоморфного шифрования.

Ранние исследования

Концепция гомоморфного шифрования была впервые предложена в 1978 году Рональдом Ривестом, Леонардом Адлеманом и Майклом Дертузосом. Они описали возможность выполнения арифметических операций над зашифрованными данными.

1

2

Прорыв в 2009 году

В 2009 году Крэйг Геннаро, Роки Геннаро и Вангее Лу представили первую практическую схему частично гомоморфного шифрования, которая могла эффективно выполнять ограниченные вычисления над зашифрованными данными.

3

Разработка полностью гомоморфного шифрования

В 2010 году Крэйг Геннаро, Сальваторе Джованни Валенте и Даниэль Вичерс описали первую схему полностью гомоморфного шифрования, которая может выполнять любые вычисления над зашифрованными данными.

Основные типы гомоморфного шифрования

- Полностью гомоморфное шифрование (Fully Homomorphic Encryption, FHE). Данный тип шифрования подразумевает возможность выполнять широкий спектр математических операций над зашифрованными данными, обеспечивает высочайший уровень безопасности и конфиденциальности, поскольку данные могут оставаться зашифрованными на протяжении всего процесса вычислений, однако алгоритмы полностью гомоморфного шифрования обладают высокой вычислительной сложностью, что существенно понижает производительность информационных систем, использующих данный тип шифрования.
- Гомоморфное шифрование с ограниченной полнотой (Somewhat Homomorphic Encryption, SHE). Данный тип шифрования позволяет выполнять ограниченное количество математических операций (сложение и умножение) над зашифрованными данными до накопления определенного уровня шума.
- Частичное гомоморфное шифрование (Partial Homomorphic Encryption). Данный тип шифрования подразумевает возможность выполнять только один тип операции над зашифрованными данными, например, сложение или умножение. Шифрование такого типа осуществляют такие распространенные алгоритмы, как RSA, Криптосистема Голдвассера-Микали, Криптосистема Эль-Гамаля, криптосистема Пэйе.

Наиболее распространенными на практике являются частично гомоморфные шифры, допускающие либо сложение, либо умножение, поскольку они обладают более низкой вычислительной сложностью, а так же более просты в реализации.

Криптосистема Пэйе

- Криптосистема Пайе (Paillier's cryptosystem) — это асимметричная криптосистема с открытым ключом, разработанная Паскалем Пайе в 1999 году. Она основана на вычислительной сложности задачи факторизации составного числа, являющегося произведением двух простых чисел. Одной из отличительных черт данной системы является возможность выполнения гомоморфных операций сложения над зашифрованными данными.

Давайте рассмотрим данный алгоритм шифрования.

1. Генерация ключей

- 1. Выбираем два простых числа p и q.
- 2. Вычисляем произведение этих числе n = p * q
- вычисляем λ = lcm(p-1, q-1), где lcm – наименьшее общее кратное.
- Выбираем случайное число g, такое, что $g \in z_{n^2}^*$
- Вычисляем μ:
  - $\mu = \left(L\left(g^{\lambda} \bmod n^2\right)\right)^{-1} \bmod n$
  - Где $L(u) = \operatorname{div}\left(\frac{u-1}{n}\right)$
  - Div – целочисленное деление.

Открытым ключом является пара (n, g), закрытым – (λ, μ).

2. Шифрование

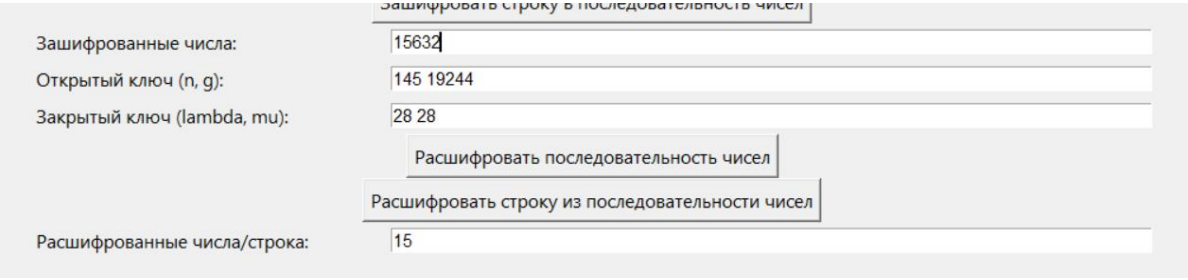
- 1. Пусть m будет шифруемым сообщением, где m ∈ z_n .
- 2. Выбор случайного числа r, r ∈ z_n^*
- 3. Вычисление шифротекста c:
  - c = $g^n * r^n \, mod \, n^2$

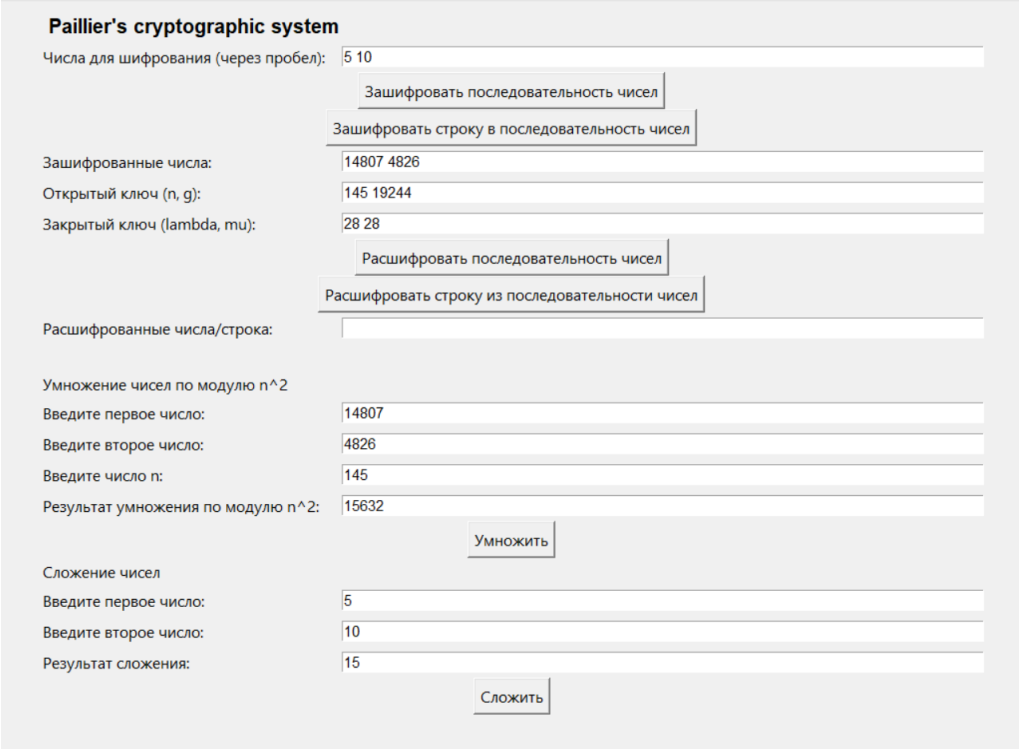
3. Расшифровка

- 1. Принимаем зашифрованное сообщение c ∈ $z^*_{n^2}$, открытый (n, g) и закрытый (λ, μ) ключи.
- 2. Вычисляем исходное сообщение по формуле:
- $m = \left(L\left(c^{\lambda} \bmod n^2\right) * \mu\right) \bmod n$

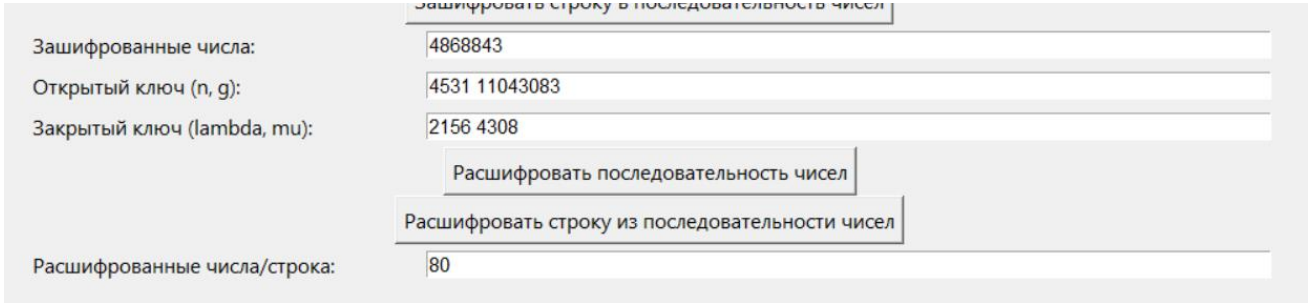
Результаты проведенной мною реализации данной криптографической системы

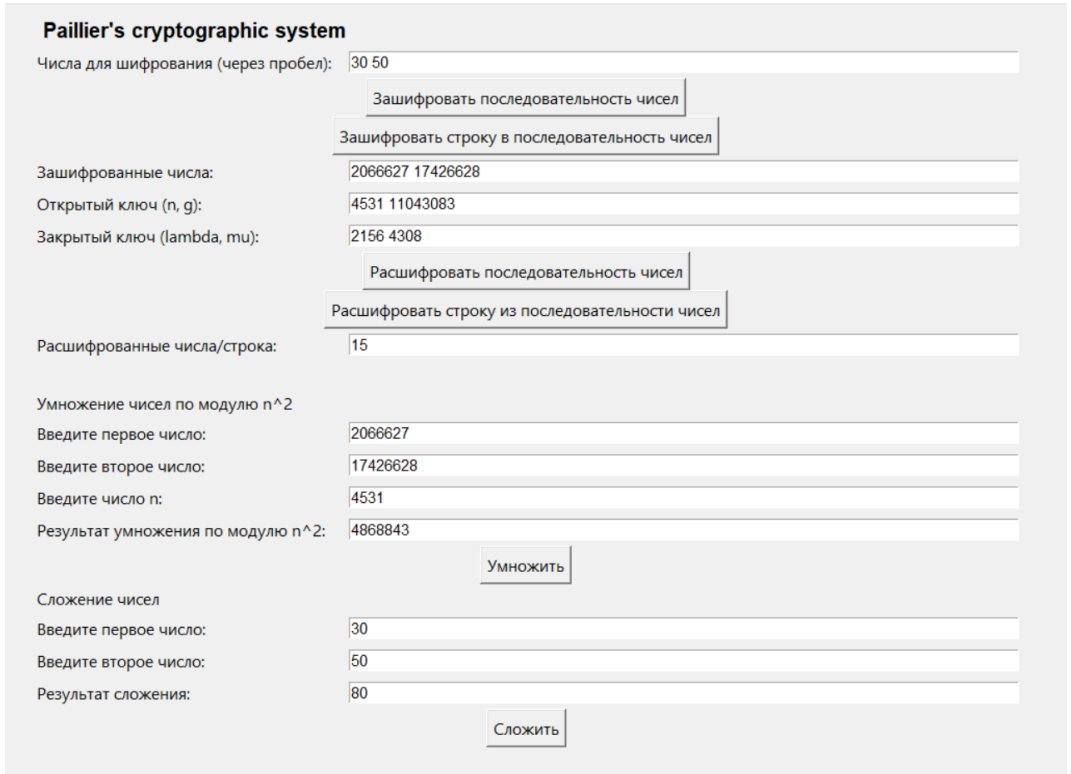
Демонстрация созданной программы



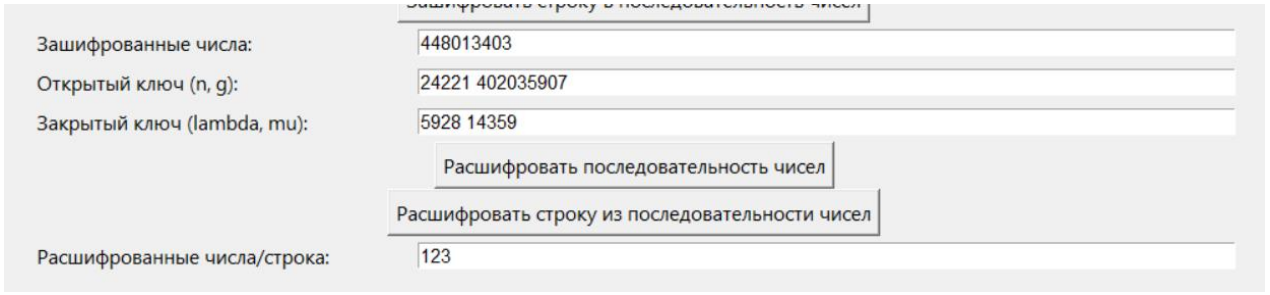


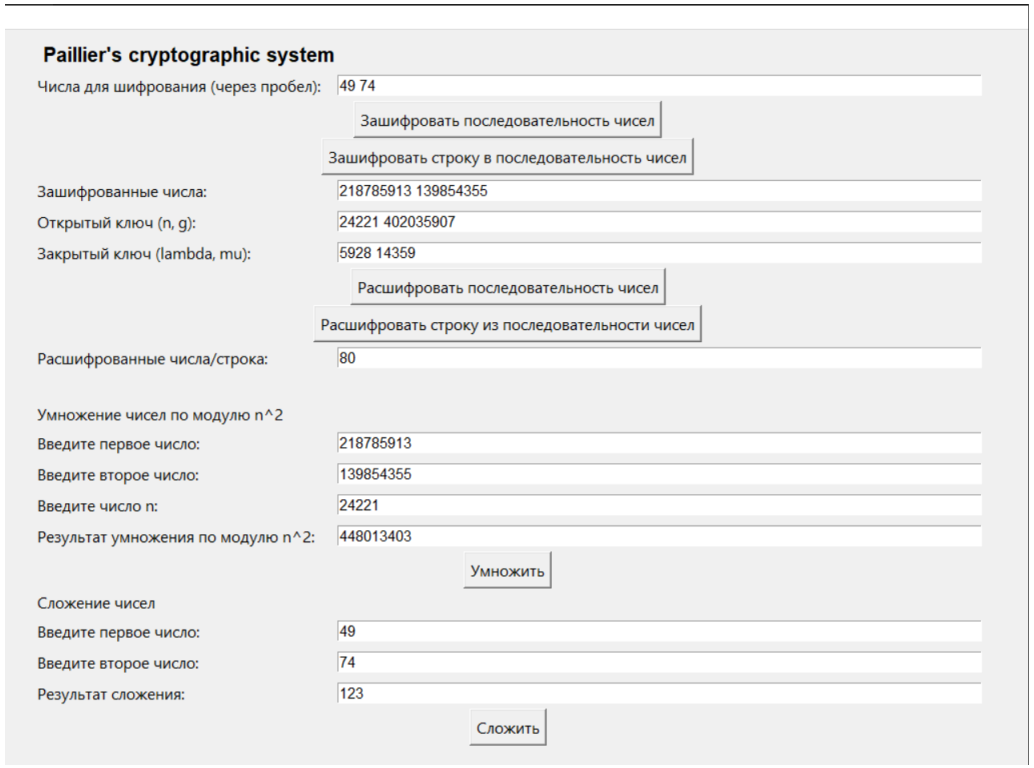
Демонстрация созданной программы



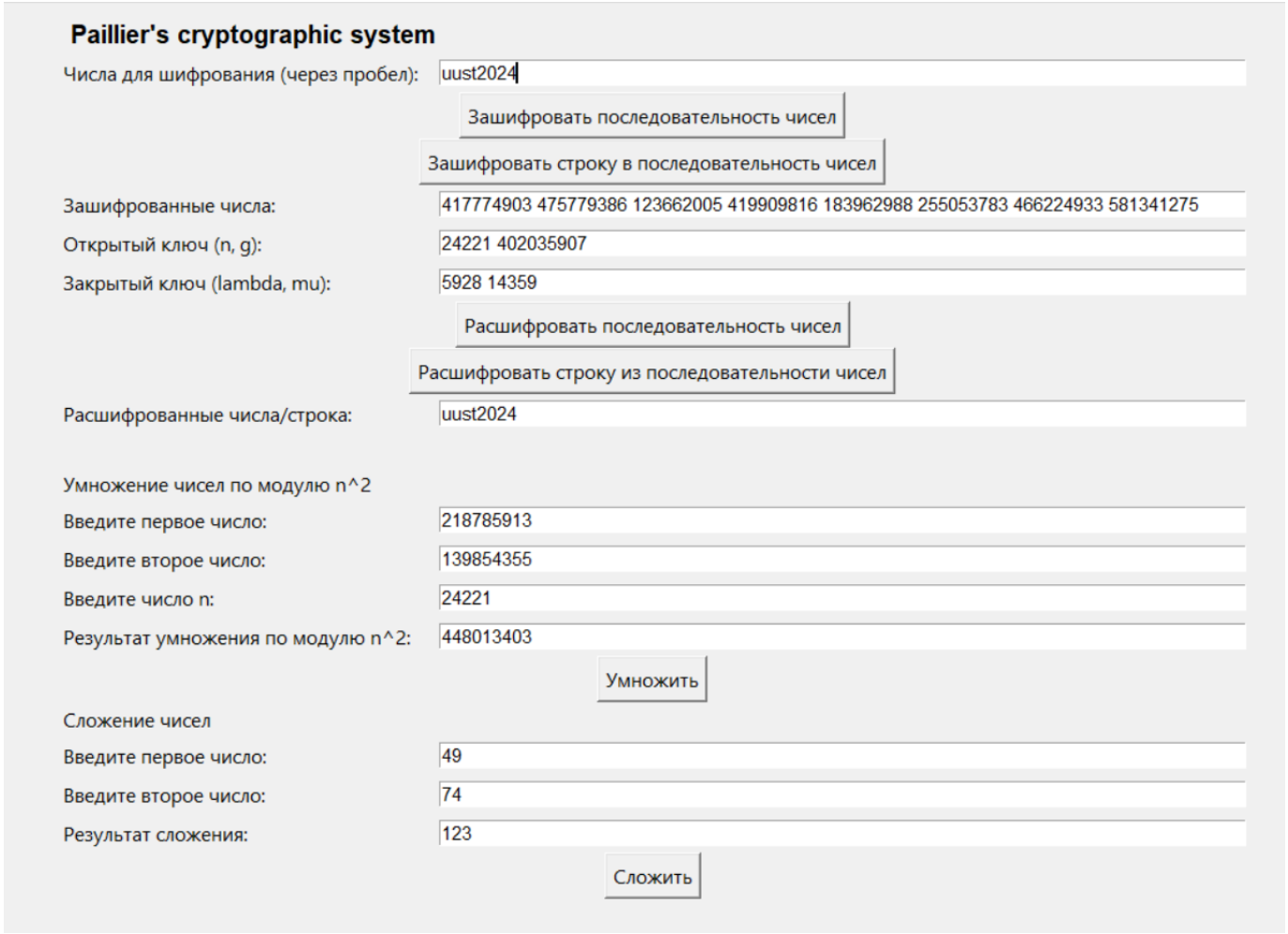


Демонстрация созданной программы





Демонстрация созданной программы



Заключение

- Гомоморфное шифрование – это перспективная технология, открывающая новые возможности для безопасной обработки данных. Несмотря на текущие проблемы с производительностью, активные исследования и разработки в данной области позволяют надеяться на широкое применение этой технологии в будущем. Обеспечение конфиденциальности данных становится все более важным в современном мире, и гомоморфное шифрование может сыграть ключевую роль в решении этой проблемы

Спасибо за внимание!