МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ Н.Г. ЧЕРНЫШЕВСКОГО»

Кафедра теоретических основ компьютерной безопасности и криптографии

Сравнительный анализ схем шифрования с открытым ключом

АВТОРЕФЕРАТ
дипломной работы

студента 6 курса 631 группы
специальности 10.05.01 Компьютерная безопасность
факультета компьютерных наук и информационных технологий
Полякова Максима Сергеевича

Научный руководитель
д.ф.-м.н., профессор _____ В. А. Молчанов
23.01.2021 г.

Заведующий кафедрой
д. ф.-м. н., доцент _____ М. Б. Абросимов
23.01.2021 г.

Саратов 2021

ВВЕДЕНИЕ

Введение криптографии с открытым ключом Уитфилдом Диффи и Мартином Хеллманом в 1976 году стало важным переломным моментом в истории криптографии. Их работа вызвала интерес в криптографическом исследовательском сообществе, и вскоре были предложены и реализованы многочисленные схемы шифрования с открытым ключом, каждая из которых опирается на сложность классической математической задачи, такой как проблема целочисленной факторизации, проблема дискретного логарифма и т.д. Для решения этих проблем на протяжении многих лет разрабатывались субэкспоненциальные алгоритмы. В результате размеры ключей стали превышать 1000 бит, для достижения разумного уровня безопасности.

Схема Ривеста, Шамира и Адлемана (RSA), являющаяся первой реализацией абстрактной модели, и сегодня остается наиболее широко используемой схемой шифрования с открытым ключом.

Цель работы – провести сравнительный анализ основных параметров следующих известных криптосистем с открытым ключом: RSA, DSA, схема Эль-Гамаля, схема Блюма-Гольдвассер, протокол Диффи-Хеллмана.

Решаемые задачи:

1) рассмотреть теоретико-числовые задачи, на основе которых строятся известные криптосистемы с открытым ключом;

2) изучить алгоритмы построения известных криптосистем с открытым ключом;

3) разработать программный комплекс на языке программирования Kotlin для реализации и сравнительного анализа рассматриваемых криптосистем;

4) реализовать графический интерфейс пользователя программного комплекса с помощью вспомогательной библиотеки TornadoFX;

5) провести оценку производительности алгоритмов на основе сравнения времени выполнения следующих операций: генерации ключей, шифрования и расшифрования, а также сравнения размера зашифрованных данных;

6) для протоколов обмена ключами оценить скорость распределения сеансовых ключей.

Дипломная работа состоит из введения, 4 разделов, заключения, списка использованных источников и 2 приложений. Общий объем работы – 167 страниц, из них 72 страниц – основное содержание, включая 67 рисунков и 17 таблиц, список использованных источников из 20 наименований.

КРАТКОЕ СОДЕРЖАНИЕ

В первом разделе дипломной работы рассматриваются элементы теории чисел и теории групп. Данный раздел содержит 4 подраздела. В первом подразделе рассматривается понятие и свойства делимости, а также алгоритмы Евклида. Второй подраздел посвящен основам теории групп. В третьем подразделе рассматриваются алгоритмы нахождения первообразного корня. В четвертом подразделе описываются задачи факторизации целых чисел и дискретного логарифмирования, на которых базируются, рассматриваемые криптосистемы.

Второй раздел посвящен криптосистемам с открытым ключом. Этот раздел содержит пять подразделов. Первый подраздел содержит информацию о криптосистеме RSA, в нем рассматриваются основные операции криптосистемы такие как: генерация ключа, шифрование, расшифрования, подписание сообщения, верификация подписи. Во втором подразделе рассматривается криптосистема DSA и основные операции этой криптосистемы: генерация ключа, подписание сообщения, верификация подписи. В третьем подразделе описывается схема Эль-Гамаля и ее небольшие сходства в алгоритмах подписания сообщения и верификации со схемой DSA. Также в этом подразделе рассматриваются операции: генерация ключа, шифрования и расшифрования. В четвертом подразделе описывается протокол обмена сеансовыми ключами Диффи-Хеллмана и его основные операции: генерация ключа и генерация сеансового ключа. В пятом подразделе рассматривается криптосистема Блюма-Гольдвассер и операции, которые позволяет производить эта криптосистема: генерация ключа, шифрование, расшифрование.

В третьем разделе дипломной работы рассматривается программная реализация криптосистем с открытым ключом, а также описывается, с помощью каких технологий был реализован программный комплекс. Первый

подраздел описывает как удобным образом с помощью программного комплекса сгенерировать открытый текст для алгоритмов. Второй подраздел описывает, как сгенерировать ключи для криптосистем и в каком виде они будут представлены для пользователя. Третий подраздел содержит примеры шифрования и подробным образом объясняет, как пользоваться этой операцией в программном комплексе. Четвертый подраздел описывает работу операции расшифрования для схем шифрования с открытым ключом. В пятом подразделе рассматривается операция подписания сообщения для алгоритмов цифровых подписей. На примерах показано, как пользоваться этой операцией. В шестом подразделе описывается операция верификации подписи. В седьмом подразделе описывается, процесс сравнения криптосистем, а также функция экспорта результатов автоматизированного анализа в excel-файл.

В четвертом разделе описывается сравнительный анализ криптосистем с открытым ключом. Этот раздел состоит из 3 подразделов, в первом из которых рассматривается сравнительный анализ для схем шифрования. В представлены результаты сравнения с числом раундов 1 и 100 (размер входных данных: 10 и 100 байт), объясняется разница в результатах, а также приводятся графики зависимостей времени выполнения операций: шифрования, расшифрования, генерации ключа от длины ключа, а также зависимость размера криптограммы от размера ключа. В конечном итоге строятся гистограммы, которые отражают преимущества и недостатки схем шифрования. Во втором подразделе представлены результаты сравнения алгоритмов цифровой подписи для входного сообщения размером 100 байт с числом раундов 1 и 100. Приводятся графики зависимостей от длины ключа времени выполнения операций: подписания сообщения, верификации подписи и генерации ключа, а также зависимость от длины ключа размера подписанного сообщения. В итоге делается вывод об алгоритмах цифровой подписи на основании гистограмм, которые были построены в ходе автоматизированного анализа. В третьем разделе представлены результаты сравнения протоколов обмена ключами для

входного сообщения размером 100 байт с числом раундов 1 и 100. Строятся графики зависимостей от длины ключа: времени генерации ключа и времени обмена сеансовым ключом, а также делается вывод об оценке времени распределения сеансовых ключей. Для протоколов обмена ключами строятся гистограммы, которые наглядным образом отражают результаты анализа.

В результате работы был произведен анализ схем шифрования. Для этого строились гистограммы, представленные на рисунках 1-2. Значения для графика 1 были получены с помощью автоматизированного анализа программного комплекса и представлены в таблице 1. В данном случае: для каждой длины ключа от 512 до 3072 с количеством раундов 100 вычислялись средние значения времени выполнения каждой операции для каждой схемы шифрования, которые затем нормировались с помощью деления на наименьшее из этих значений. В результате «наилучшая» криптосистема будет иметь значение 1, а у остальных криптосистемы будут значения > 1, показывающие во сколько раз они «хуже» наилучшей.

Наконец для графика 2, вычисляется сумма полученных средних для всех показателей криптосистем и проводится такая же нормировка (делением на наименьшее) для определения «наилучшей» криптосистемы с учетом всех операций, а остальные значения будут показывать, во сколько раз соответствующие криптосистемы «хуже» наилучшей. Отметим, что программа позволяет также сравнивать взвешенные суммы всех показателей криптосистем с коэффициентами $0 \leq k \leq 1$, определяющими важность рассматриваемых показателей для криптосистем с открытым ключом.

Таблица 1 – Оценка эффективности схем шифрования для различных операций

Схема шифрования	Операция					
	Шифрование	Расшифрование	Размер шифрограммы	Генерация ключа	Сумма	Нормир. сумм.
RSA	1	130	1	1	133	19,9
ELGAMAL	603	135	40,7	6,85	785,55	117,2
Blum–Goldwasser	2,74	1	1	1,96	6,7	1

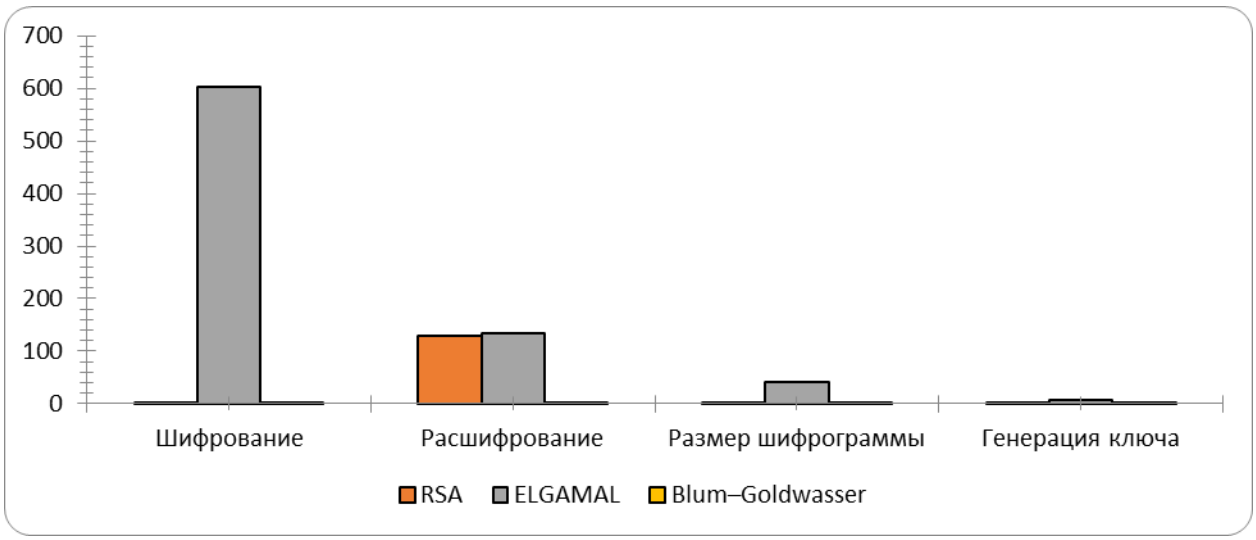

Рисунок 1 – Оценка эффективности схем шифрования для различных операций

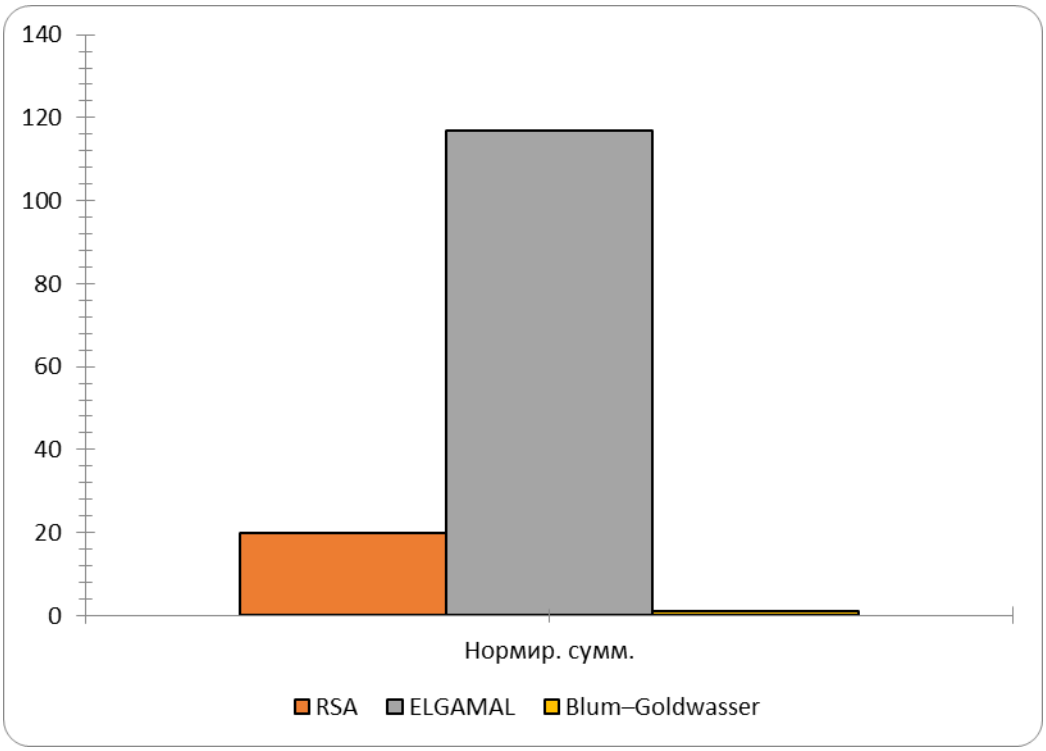

Рисунок 2 – Оценка лучшей схемы шифрования с учетом всех операций

На основе экспериментов было замечено, что RSA очень эффективен при шифровании, но медленен при расшифровании, это обусловлено тем, что открытая экспонента много меньше, чем закрытая экспонента, которая используется при расшифровании, при этом процедуры шифрования и расшифрования представлены в виде операции возведения в степень.

Схемы RSA и Эль-Гамаля показывают одинаковую скорость при расшифровании. Хорошо видно, что при генерации ключа (при 1 раунде) для

схемы Эль-Гамаля наблюдаются скачки на графиках, это обусловлено тем, что алгоритм генерации зависит от генерации первообразного элемента, который в свою очередь зависит от факторизации чисел. Факторизация может работать в некоторых ситуациях быстрее, в некоторых дольше, но при 100 раундах график без явных скачков, но производительность хуже по той же причине.

При схеме Эль-Гамаля шифрограмма имеет заметно больший размер, чем при шифровании другими схемами.

Генерация ключа у данных схем шифрования приблизительно одинаковая.

Из рисунков 1-2 хорошо видно, что схема Блюма-Гольдвассер имеет преимущество перед остальными криптосистемами по всем показателям. Наихудшим образом, с учетом всех операций, проявила себя схема Эль-Гамаля.

В ходе работы также был произведен анализ алгоритмов цифровой подписи. Для этого строились гистограммы, представленные на рисунках 3-4. Значения для графика 3 были получены с помощью автоматизированного анализа программного комплекса и представлены в таблице 2.

Таблица 2 – Оценка эффективности цифровых подписей для различных операций

Схема шифрования	Операция					
	Подпись	Верификация	Размер подписи	Генерация ключа	Сумма	Нормир. сумм.
RSA	308	1	13	21	343	8,33
DSA	1	38,2	1	1	41,2	1
ELGAMAL	23,2	571	13,3	138	745,5	18,1

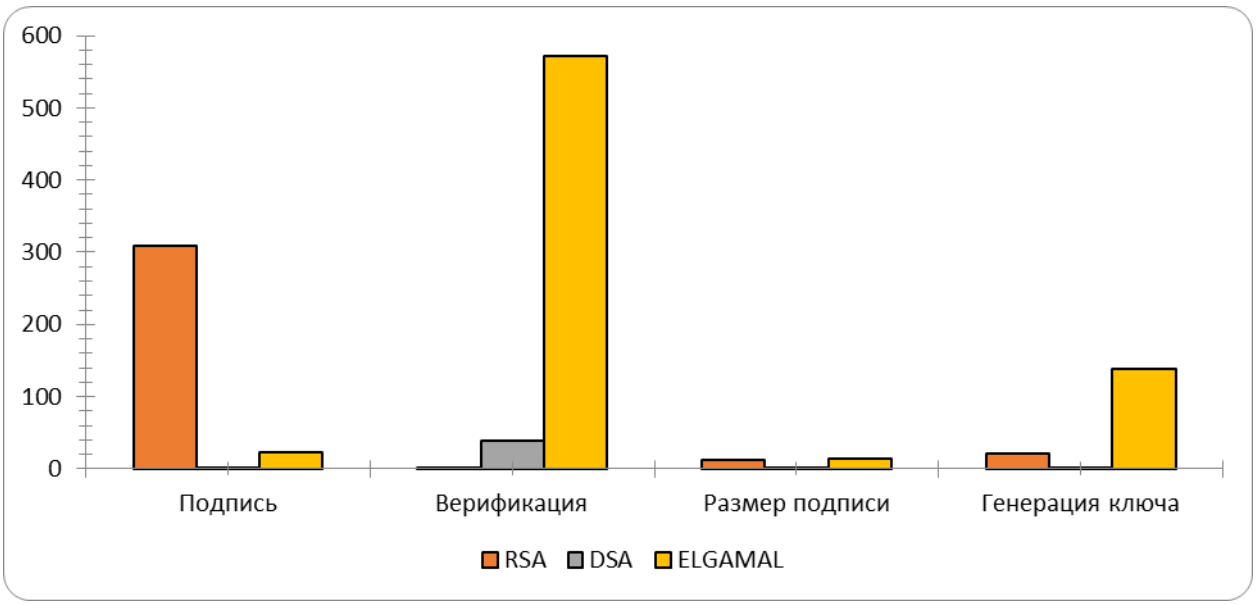

Рисунок 3 – Оценка эффективности алгоритмов цифровых подписей для различных операций

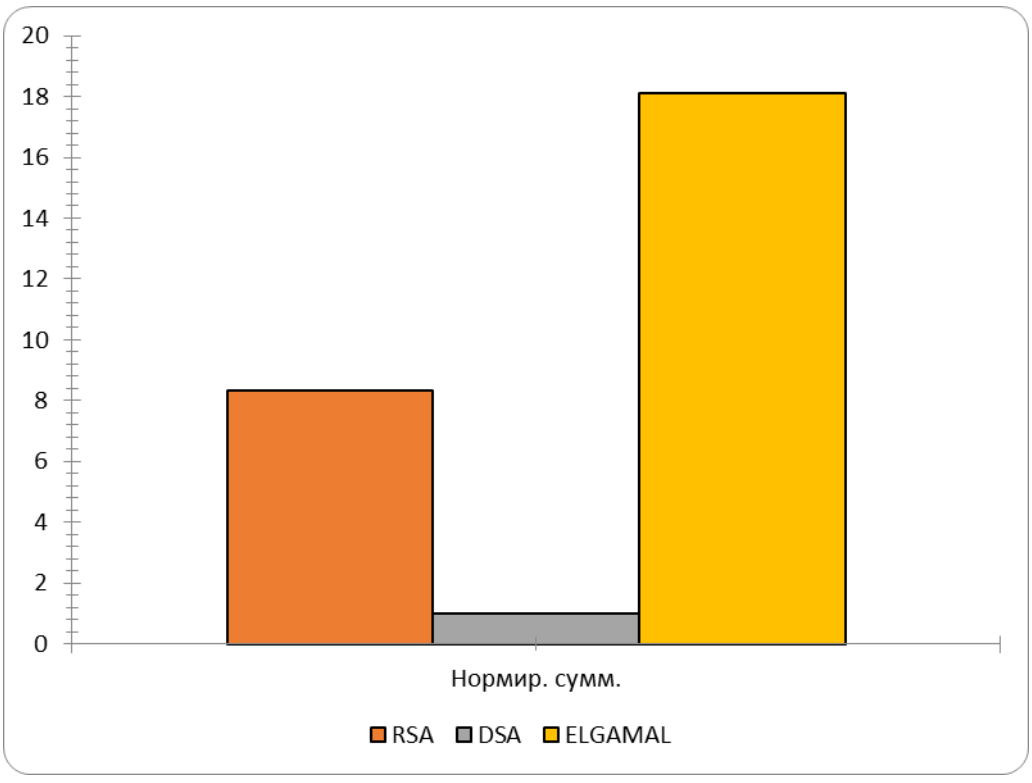

Рисунок 4 – Оценка лучшей схемы цифровой подписи с учетом всех операций

Судя по графикам, хуже себя по скорости подписания сообщения показывает RSA, это связано с тем, что при подписании используется закрытая экспонента, которая много меньше открытой, отсюда вытекает, что схем RSA очень хорошо показывает себя при операции верификации, опережая все алгоритмы. При верификации самый плохой результат показывает схема Эль-

Гамаля. При подписании хорошую сверточную способность показывает алгоритм DSA, его подпись меньше всего занимает места на диске. Остальные алгоритмы имеют приблизительно одинаковый размеры цифровых подписей. Во время генерации ключей видны скачки у схемы Эль-Гамаля (для 1 раунда), причину рассмотрели в разделе выше.

Из рисунка 4 хорошо видно, что алгоритм DSA имеет преимущество перед остальными схемами по всем показателям. Наихудшем образом, с учетом всех операций, проявила себя схема Эль-Гамаля, так же, как и при оценке схем шифрования.

Заметим, что для некоторых значений длинны ключа нет соответствующих характеристик. Это обусловлено тем, что стандарт DSA не позволяет генерировать ключи данных размеров, об этом было написано в разделе 2.2 дипломной работы. Выбор диапазона размера ключей (512-1024 бит) выбран именно по этой причине. Ключи можно сгенерировать на этом диапазоне в том случае, если размер ключа кратен 64 битам. Если размера ключа ниже 512 битов – стандарт не позволяет сгенерировать ключ.

Заключительной частью анализа являются протоколы обмена сеансовыми ключами. Для этого строились гистограммы, представленные на рисунках 5-6. Значения для графика 5 были получены с помощью автоматизированного анализа программного комплекса и представлены в таблице 3.

Таблица 3 – Оценка эффективности протоколов обмена ключами для различных операций

Схема шифрования	Операция			
	Обмен сеансовыми ключами	Генерация ключей	Сумма	Нормир. сумм
RSA	32,9	1	33,9	4,44
DIFFIE-HELLMAN	1	6,63	7,63	1

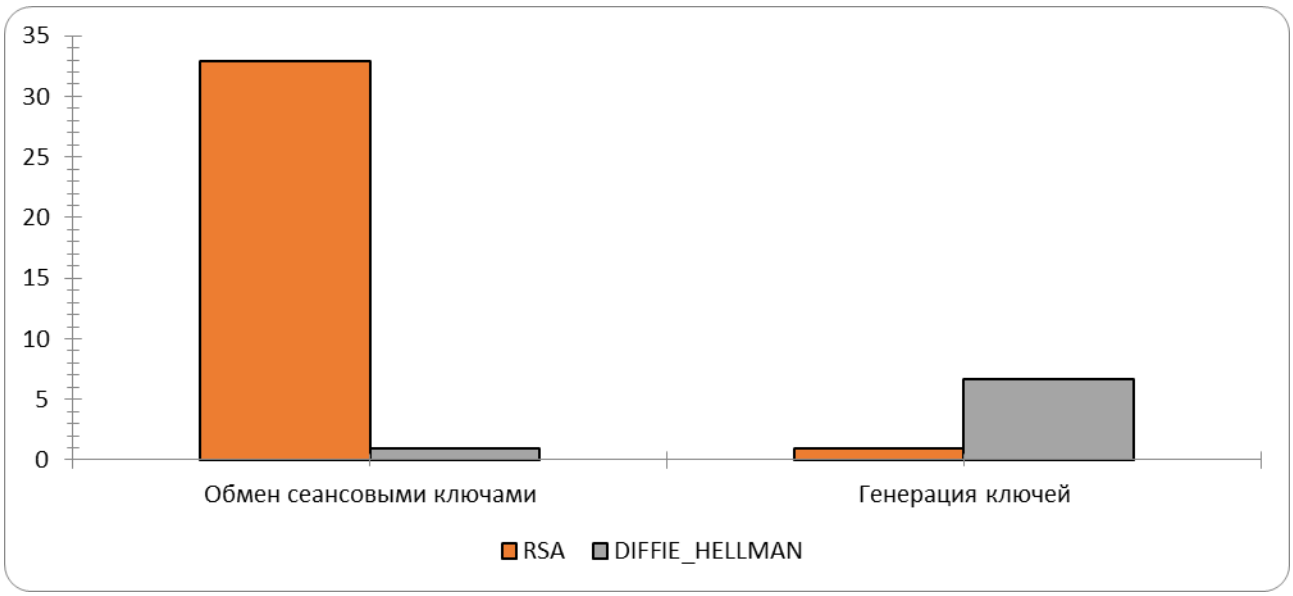

Рисунок 5 – Оценка эффективности протоколов обмена ключами для различных операций

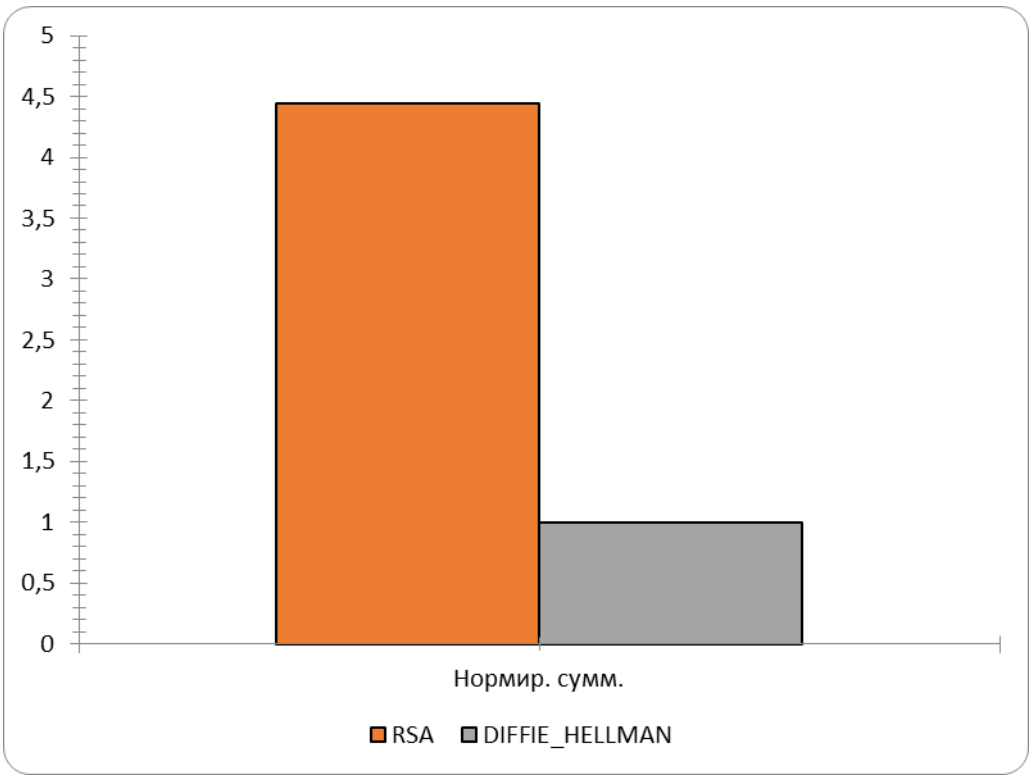

Рисунок 6 – Оценка лучшего протокола обмена ключами с учетом всех операций

Из рисунка 5 видно, что схема Диффи-Хеллмана тратит больше времени на генерацию ключей для протокола, но в процессе обмена сеансовыми ключами она показывает хороший результат по времени, превосходящий схему RSA в несколько раз.

ЗАКЛЮЧЕНИЕ

В ходе работы изучены алгоритмы известных криптосистем с открытым ключом такие как: RSA, DSA, схема Эль-Гамаля, схема Блюма-Гольдвассер, протокол Диффи-Хеллмана, а также рассмотрены теоретико-числовые задачи, на основе которых строятся рассматриваемые криптосистемы.

В практической части работы разработан программный комплекс на языке программирования Kotlin для реализации и сравнительного анализа рассматриваемых криптосистем. Для удобства использования программного комплекса разработан пользовательский интерфейс с помощью вспомогательной библиотеки TornadoFX, который позволяет удобно взаимодействовать с приложением и выполнять необходимые операции. Программный комплекс позволяет производить оценку производительности алгоритмов на основе сравнения времени выполнения следующих операций: генерации ключей, шифрования и расшифрования, а также сравнения размера зашифрованных данных. Для протоколов обмена ключами программный комплекс позволяет производить оценку времени распределения сеансовых ключей.

В дополнение к этому пользователю доступна функция экспорта результатов автоматизированного анализа в отдельные excel-файлы, которые содержат таблицы и графики сравнения для каждой операции. При этом на отдельной вкладке доступен анализ криптосистем с учетом всех операций, который отражается наглядными гистограммами.

Поставленные задачи полностью решены.

Программный комплекс может применяться в учебных целях, а также в прикладных задачах, связанных с разработкой и анализом криптосистем с открытым ключом.