### Министерство науки и высшего образования Российской Федерации

1. Санкт-Петербургский политехнический университет Петра Великого
2. —
3. Институт компьютерных наук и кибербезопасности
4. Высшая школа кибербезопасности

**ЛАБОРАТОРНАЯ РАБОТА № 2**

1. **«Атаки на криптосистему RSA, использующие**
2. **данные о показателях»**
3. по дисциплине «Криптографические методы защиты информации»
4. Выполнил
5. студент гр. 5151001/00201 Устюгов А. А.

<*подпись*>

1. Проверил:
2. старший преподаватель, к.т.н. Тулинова А. В.

<*подпись*>

1. Санкт-Петербург
2. 2024

# Цель работы

Изучение уязвимостей криптосистемы RSA по отношению к атакам, использующим показатели, обладающие определенными свойствами, генерация параметров криптосистемы RSA.

# Порядок выполнения работы

1. Разработать программу П-1, которая реализует разложение составного числа на множители по известным показателям RSA и вычисляет закрытый ключ другого пользователя в случае общего модуля 𝑛. Программа П-1 должна принимать на вход открытый и закрытый ключ RSA, а также открытый ключ RSA другого пользователя; на выходе – возвращать множители модуля RSA, закрытый ключ другого пользователя.
2. Разработать программу П-2, которая реализует атаку Винера на криптосистему RSA. Программа П-2 должна принимать на вход открытый ключ RSA: число 𝑛 и показатель 𝑒; на выходе – возвращать закрытый показатель 𝑑.
3. Разработать программу П-3, реализующая бесключевое дешифрование сообщения в случае малого порядка элемента 𝑒 в группе ()\*. Программа П-3 должна принимать на вход открытый ключ RSA, шифр текст; на выходе – возвращать восстановленный открытый текст
4. Разработать программу П-4, которая осуществляет генерацию параметров криптосистемы RSA. Разработка процедур генерации случайных чисел и проверки числа на простоту не требуется. Генерация ключей должна обеспечивать выработку безопасных параметров криптосистемы с учетом произведенных атак. Программа П-4 должна принимать на вход битовую длину модуля RSA; на выходе – возвращать параметры криптосистемы: 𝑛, 𝑒, 𝑑. Выполнить анализ сгенерированных параметров с помощью инструмента CrypTool.

# Ход работы

Наличие атак на криптосистему накладывает значительные ограничения на выбор параметров. Рассмотрим несколько существующих атак и определим ограничения параметров криптосистемы для их предотвращения.

1. **Случай общего модуля**

Если в системе RSA у пользователей 𝐴 и 𝐵 общее составное число 𝑛, но различные открытые 𝑒𝐴, 𝑒𝐵 и закрытые 𝑑𝐴, 𝑑𝐵 показатели, где 𝑒𝐴𝑑𝐴 ≡ 𝑒𝐵𝑑𝐵 ≡ 1(𝑚𝑜𝑑 𝜑(𝑛)), то каждый пользователь может разложить число 𝑛 на множители и тем самым узнать закрытый ключ другого пользователя.

Для этого достаточно найти квадратный корень из единицы, отличный от ±1. Если 𝑡2 ≡ 1 (𝑚𝑜𝑑 𝑛), 𝑡 ≠ ±1 (𝑚𝑜𝑑 𝑛), то выполняется сравнение

𝑡2 − 1 = (𝑡 + 1)(𝑡 − 1) ≡ 0 (𝑚𝑜𝑑 𝑛)

В таком случае числа 𝑡 + 1, 𝑡 − 1 имеют нетривиальные общие делители с 𝑛.

1. **Случай малого закрытого показателя**

Атака Винера на схему RSA основана на предположении о том, что значение закрытого показателя 𝑑 достаточно мало.

Пусть 𝑛 = 𝑝𝑞, 𝑞 < 𝑝 < 2𝑞, (𝑛, 𝑒) − открытый ключ, (𝑛, 𝑑) − закрытый ключ схемы RSA. Тогда если

,

то значение закрытого показателя 𝑑 может быть вычислено за полиномиальное от 𝑛 время.

Для доказательства этого предположения используется математический аппарат непрерывных дробей.

Открытый и закрытый показатели связаны соотношением 𝑒𝑑 ≡ 1 (𝑚𝑜𝑑 𝜑(𝑛)), т. е. существует такое 𝑘 ∈ ℤ, что 𝑒𝑑 = 1 + 𝑘𝜑(𝑛), или |𝑒𝑑 − 𝑘𝜑(𝑛)| = 1.

Подходящая дробь со знаменателем, близким к , является хорошим приближением к . Действуя таким образом, можно найти закрытый показатель 𝑑, если его длина достаточно мала.

1. **Случай специальных открытых показателей**

Aтака на схему шифрования возможна, если мал порядок элемента 𝑒 в группе ()\*. Для нахождения сообщения 𝑚 по шифртексту необходимо выполнить последовательное зашифрование шифртекста , и т. д. до получения шифртекста 𝑐, тогда предыдущее значение и будет открытым текстом.

1. **Генерация безопасных параметров RSA**

На основе изученных атак была реализована процедура, генерирующая относительно безопасные параметры криптосистемы рекомендуемого размера 1024 бит.

При генерации параметров выполняются следующие условия:

* Не допускается малое значение показателя e
* Не выполняется неравенство, допускающее атаку Винера
* Числа p-1 и q-1 имеют большие простые делители
* Числа p и q имеют одинаковую битовую длину, но находятся не близко по отношению друг к другу, нарушая атаку Ферма

Сгенерированные параметры были проанализированы с помощью утилиты CrypTool. Утилита CrypTool предоставляет широкий набор инструментов для изучения принципа действия различных криптосистем, визуализации атак, генерации и тестирования параметров.

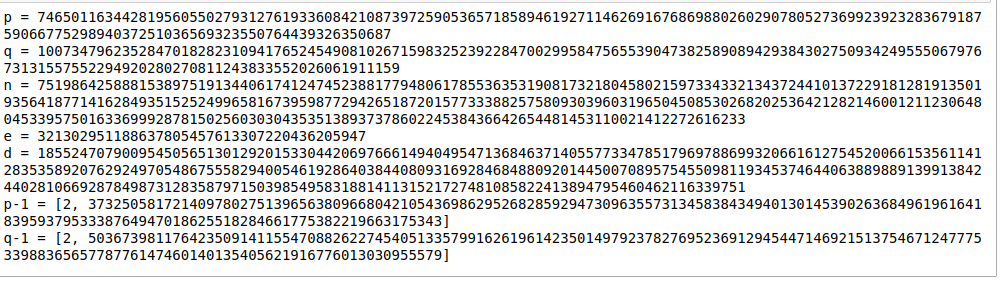


Рисунок 1 – сгенерированные параметры

При проверке сгенерированных значения инструмент СrypTool не смог получить разложение для n за приемлемое время.

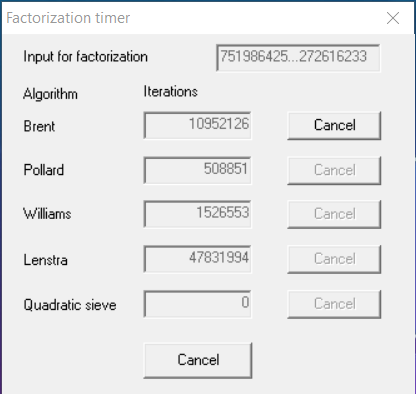


Рисунок 2 – разложение полученного n с помощью CryptTool

# Ответы на контрольные вопросы

**1. При каком условии возможна атака Винера?**

Атака Винера на схему RSA основана на предположении о том, что значение закрытого показателя 𝑑 достаточно мало, а именно:

**2. Перечислите методы противодействия атаке Винера.**

В первую очередь, избегать выполнения неравенства (1) при генерации параметров криптосистемы.

Также предлагается использовать большее значение е’ следующего вида:

При использовании большего значения e’, значение k перестает быть малым:

Таким образом, подходящая дробь 𝑘/𝑑 уже не является достаточно хорошим приближением к 𝑒/𝑛 . Расчет показывает, что, если e’ > n1,5, то независимо от того, как бы ни было мало d, описанная выше атака Винера становится невозможна. Однако, использование большого значения открытого показателя приводят к увеличению времени шифрования.

**3. Почему числа 𝑝 и 𝑞 необходимо выбирать так, чтобы 𝑝 − 1, 𝑞 − 1 имели большие простые делители?**

Для того, чтобы усложнить задачу факторизации с помощью (p – 1) метода Полларда.

**4. Предложите способы защиты от атаки бесключевого дешифрования широковещательных сообщений без отказа от использования общих малых закрытых показателей.**

В общем случае, если все открытые показатели равны e, злоумышленник может восстановить сообщение M, как только количество сообщений k превысит или станет равным значению e.

Таким образом, малый открытый показатель нужно выбирать таким образом, чтобы число широковещательных сообщений не достигало его значения.

# Вывод

В данной лабораторной работе были изучены и реализованы основные атаки на криптосистему RSA, определены ограничения для генерации параметров криптосистемы для предотвращения изученных атак.

С учетом произведенных атак была реализована процедура, генерирующая «безопасные» параметры RSA относительно исследуемых атак, анализ которых был произведён с помощью инструмента CrypTool.