ОБУЧАЮЩАЯ ПРОГРАММА ДЛЯ АНАЛИЗА КРИПТОСТОЙКОСТИ ШИФРА

КОРОЛЬКОВ Иван Денисович
студент
Иркутский государственный университет
г. Иркутск, Россия

Статья рассматривает возможности программы Gamma в обучении студентов анализу крипкостойкости шифра гаммирования. Описаны свойства разработанного интерфейса и функционал программы, эффективно влияющие на обучение и способствующие развитию критического мышления и аналитических навыков.

Ключевые слова: криптография, криптоанализ, гаммирование, гамма, интерфейс, функция, частотный анализ, обучение студентов.

В обучении криптоанализу особое внимание следует уделять не только теоретическим знаниям, но и практическим навыкам, которые способствуют глубокому пониманию механизма работы криптографических систем. Важным аспектом является то, что инструменты для практического обучения не должны выполнять работу за студентов, а лишь обеспечивать вспомогательные функции, облегчая процесс анализа и позволяя фокусироваться на ключевых аспектах криптоанализа. Таким образом, студенты получают возможность самостоятельно исследовать и интерпретировать процессы шифрования, развивая критическое мышление и навыки, необходимые для решения реальных задач в области криптографии и информационной безопасности. Разработанный интерфейс программы Gamma для обучения студентов анализу криптостойкости шифра гаммирования соответствует этому подходу, обеспечивая студентам поддержку в их исследовательской деятельности, но оставляя пространство для самостоятельного анализа и принятия решений.

Шифр гаммирования – это один из самых распространенных и понятных методов симметричного шифрования, основанный на побитовом сложении открытого текста с псевдослучайным ключом (гаммой), который имеет такую же длину, как и сам текст. Гамма генерируется с использованием ключа, а затем каждый бит или символ исходного сообщения комбинируется с соответствующим элементом гаммы, что приводит к зашифрованному тексту. Благодаря своей простоте и прозрачности в механизмах шифрования и дешифрования, шифр гаммирования является отличным средством для обучения студентов основам криптографии и криптоанализа, предоставляя возможность на практике изучить уязвимости и методы атаки на симметричные системы.

Gamma является эффективным инструментом для изучения методов анализа криптостойкости шифра гаммирования и предоставляет широкий спектр функционала, способствующего углубленному пониманию принципов криптографии [1; 2]. В интерфейсе программы заложены удобные визуальные объекты и различные вспомогательные функции.

Одной из ключевых возможностей интерфейса является выбор уровня сложности, который оказывает влияние на величину гаммы. Эта функция позволяет студентам варьировать параметры шифрования, что способствует четкому пониманию того, как изменения в алгоритмах криптографии влияют на безопасность зашифрованного текста. Студенты могут на практике наблюдать, как увеличение или уменьшение величины гаммы влияет на сложность взлома шифра, что помогает лучше понять механизмы криптостойкости.

На более лёгких уровнях сложности программа отображает варианты строк, которые с высокой вероятностью могут привести к нахождению исходного текста. Эта функция позволяет на практике исследовать возможные методы анализа криптографических систем, такие как частотный анализ и методы подбора ключа. Визуализация наиболее вероятных строк для восстановления исходного текста дает студентам наглядное пред-

ставление о том, как шифр может быть подвержен атакам.

Также в интерфейсе предоставлена возможность отслеживать и сравнивать частоту разных букв в зашифрованном и в открытом текстах. Сравнение частот символов в зашифрованных и исходных текстах помогает понять, как различные криптографические методы воздействуют на структуру текста.

На практике такой подход позволяет выявить уязвимости в криптографической системе. Например, в шифре, который плохо скрывает частотное распределение символов, криптоаналитики могут использовать методы частотного анализа для восстановления исходного текста. Возможность сравнивать частоту букв в зашифрованных и открытых текстах дает студентам отчетливое представление, как атаки на основе статистики могут быть использованы для вскрытия слабых мест в шифровании.

Перемещение между строками зашифрованного текста позволяет студентам исследовать различные фрагменты шифрованного сообщения, выявляя закономерности или аномалии в структуре шифра. Этот процесс дает возможность применять различные методы анализа или предположения о структуре текста для сужения области поиска открытого текста.

Возможность перемещаться между строками зашифрованного текста и смещать буквы на определенные позиции значительно расширяет возможности анализа криптографических систем. Функция смещения букв на определенные позиции представляет собой практическое применение методов криптографического взлома, таких как метод подбора ключа или атак с использованием смещения. Студенты могут экспериментировать с различными смещениями, что помогает им понять, как изменяются криптографические алгоритмы при варьировании ключевых параметров.

Интерфейс программы позволяет проверять правильность восстановленного открытого текста, что не только обеспечивает обратную связь, но и помогает эффективно отслеживать прогресс в процессе обучения. Если восстановление не произошло, система сообщает об этом, что мотивирует студентов продолжить работу и дает возможность применить другие методы. В случае успешного восстановления исходного текста программа уведомляет студента и предоставляет информацию о времени, затраченном на решение. Это позволяет фиксировать достигнутый результат и измерять свою эффективность и скорость работы. Студенты могут использовать эту информацию для оценки своей производительности и для оптимизации своих методов работы.

Таким образом, разработанный интерфейс и функционал программы Gamma не только облегчает обучение криптографии, но и способствует развитию критического мышления и аналитических навыков, необходимых студентам для оценки и создания устойчивых криптографических алгоритмов.

ЛИТЕРАТУРА

1. *Глухов М.М., Круглов И.А., Пичкур А.Б.* Введение в теоретико-числовые методы криптографии. – М.: Лань, 2024. – 396 с.

2. *Применко Э.А., Борисов А.В.* Алгебраические основы криптографии в задачах и упражнениях. Учебное пособие. – М.: КУРС, 2023. – 104 с.

TRAINING PROGRAM FOR ANALYSIS OF CIPHER CRYPTOCURRENCY

KOROLKOV Ivan Denisovich
Student
Irkutsk State University
Irkutsk, Russia

The article examines the capabilities of the Gamma program in teaching students to analyze the cryptographic resistance of the gamma cipher. The properties of the developed interface and the functionality of the program are described, effectively influencing learning and promoting the development of critical thinking and analytical skills.
Keywords: cryptography, cryptanalysis, gamma, interface, function, frequency analysis, student teaching.