ОБУЧАЮЩИЙ МОДУЛЬ «ИССЛЕДОВАНИЕ СТОЙКОСТИ КРИПТОСИСТЕМЫ RSA»

А.М. Деликатный

Учреждение образования «Гродненский государственный университет имени Янки Купалы», Гродно, Беларусь

В современном информационном мире обеспечение безопасности данных является одним из приоритетов. Криптосистема RSA (RSA Cryptosystem) широко используется для защиты информации, особенно в сфере финансов, коммуникаций и электронной коммерции. Однако, несмотря на свою распространенность, она подвержена различным атакам, таким как атака Винера, атака с использованием общего модуля и других [1]. Понимание этих уязвимостей крайне важно для специалистов по информационной безопасности.

В этой работе был разработан веб-сайт на фреймворке React, который может быть использован для обучения молодых специалистов атакам на криптосистему RSA. Веб-сайт предлагает доступ к лабораторным работам, состоящим как из теоретического материала, так и из практических заданий. Задания позволяют студентам углубленно изучить и применить полученные знания о криптосистеме RSA. Каждая лабораторная работа представляет собой комплексное изучение определенного аспекта криптосистемы RSA и связанных с ней уязвимостей. В теоретическом материале освещаются основы криптографии, включая принципы работы алгоритма RSA, методы шифрования и дешифрования, а также ключевые аспекты безопасности. Практические задания предлагают студентам решать реальные криптографические задачи, включая атаки на RSA, такие как атака Винера и атака с использованием общего модуля.

Веб-сайт предоставляет студентам возможность активного участия в обучении, позволяя им применять полученные теоретические знания на практике. Они могут выполнять практические задания, проверять правильность своих решений и постоянно совершенствовать свои навыки в области криптографии и кибербезопасности.

Разработка обучающего модуля по атакам на криптосистему RSA является значимым шагом в обучении специалистов по информационной безопасности. Понимание уязвимостей криптосистемы RSA и методов их защиты является ключевым элементом в обеспечении безопасности данных в современном информационном мире. Предоставление студентам возможности изучать и практиковать атаки на RSA в безопасной среде способствует их подготовке к реальным ситуациям и повышает общий уровень компетенции в области кибербезопасности.

Дальнейшее развитие обучающего модуля позволит расширить его функциональность до включения новых криптосистем и методов защиты данных. Возможность изучать не только уязвимости RSA, но и других криптографических алгоритмов позволит студентам получить более глубокие знания в области криптографии и информационной безопасности. Такой подход позволит создать полноценный ресурс для подготовки специалистов, способных эффективно защищать данные и информационные системы от различных угроз в сфере кибербезопасности.

Список литературы

1. Ян, С. Й. Криптоанализ RSA / С. Й. Ян. – Ижевск: НИЦ «Регулярная и хаотическая динамика»: Ижевский институт компьютерных исследований, 2011. – 312 с.