ПРОГРАММНОЕ СРЕДСТВО ДЛЯ РЕАЛИЗАЦИИ КРИПТОГРАФИЧЕСКИХ ОПЕРАЦИЙ

М.В. Тимошенко

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Беларусь

Чем глубже цифровые технологии проникают в нашу жизнь, тем важнее становится защита огромных объемов конфиденциальных данных. В связи с этим появляется чрезвычайная актуальность изучения криптографии, в том числе потому что она представляет собой захватывающее и важное поле, которое объединяет математику, информатику и кибербезопасность. В виртуальном пространстве криптография находит широкое применение: это неотъемлемая часть нашей цифровой жизни, в которой нам приходится постоянно заботиться о безопасности личных данных. Криптография использует некоторые низкоуровневые криптографические алгоритмы для достижения одной или нескольких из этих целей информационной безопасности. Среди этих инструментов – алгоритмы шифрования, алгоритмы цифровой подписи, алгоритмы хэширования и другие функции. Алгоритм шифрования – это процедура, которая преобразует сообщение в формате неформатированного текста в зашифрованный текст. ЭЦП (электронная цифровая подпись) – контрольная характеристика сообщения, которая вырабатывается с использованием личного ключа, проверяется с использованием открытого ключа,

служит для контроля целостности и подлинности сообщения и обеспечивает невозможность отказа от авторства. Криптографическая хэш-функция – это инструмент для преобразования произвольных данных в «отпечаток» фиксированной длины. Хэш-функции создаются таким образом, чтобы было сложно найти два различных набора входных данных, дающих один и тот же отпечаток, и чтобы было сложно найти сообщение, отпечаток которого совпадает с фиксированным значением [1].

Для реализации криптографических алгоритмов была разработана программа CryptoEtalon на фреймворке Qt [2], использующая Bee2 [3] – криптографическая библиотека, реализующая стандартизированные в Республике Беларусь криптографические алгоритмы и протоколы. CryptoEtalon – это средство проверки стандартов защиты информации, позволяющее пользователю на основе полученных данных из программы тестировать и оценивать криптографические алгоритмы на их стойкость и эффективность, оценивать совместимость между различными системами и устройствами, использующими криптографию, а так же может служить для обучающих целей: ознакомления с принципами криптографии, проверки своих знаний, реализующая следующие функции [4]:

– криптографические алгоритмы на основе sponge-функции в соответствии с СТБ 34.101.77-2020.

– алгоритмы шифрования данных и контроля целостности в соответствии с СТБ 34.101.31-2020;

– алгоритмы выработки электронной цифровой подписи в соответствии с СТБ 34.101.45-2013;

– алгоритмы генерация псевдослучайных чисел в соответствии с СТБ 34.101.47-2017;

– алгоритмы разделение секрета в соответствии с СТБ 34.101.60-2014;

– формирование общего ключа на основе эллиптических кривых в соответствии с СТБ 34.101.66-2014.

Список литературы

1. Что такое криптография? [Электронный ресурс]. – Режим доступа: https://aws.amazon.com/ru/what-is/cryptography/. – Дата доступа: 18.04.2024

2. Ot Group [Электронный ресурс]. – Режим доступа: https://www.qt.io/ – Дата доступа: 18.04.2024

3. Библиотека Bee2 [Электронный ресурс]. – Режим доступа: https://apmi.bsu.by/blog/cryptology/bee2.html. – Дата доступа: 18.04.2024

4. Национальный фонд технических нормативных правовых актов [Электронный ресурс]. – Режим доступа: https://tnpa.by/#!/SimpleSearch/search_value=криптография/tab=TabOne/page=/status=/state=/num_of_records= – Дата доступа: 18.04.2024.