Р. Э. Шишкин
10 класс, МБОУ гимназия № 7 г. Балтийск

«AMBERNETWORKER» – РАЗРАБОТКА JAVA-БИБЛИОТЕКИ ДЛЯ БЕЗОПАСНОЙ ПЕРЕДАЧИ ВАЖНОЙ ИНФОРМАЦИИ

Научный руководитель:
Ю. Ф. Болтнев — доцент кафедры компьютерной безопасности БФУ им. И. Канта.

Введение

Актуальность проблемы. В настоящее время проблема безопасности информации как никогда актуальна — утечки информации из спецслужб, международные скандалы о нарушении приватности граждан и многие другие подобные случаи дают повод веб-сайтам и мобильным приложениям переходить на защищенное соединение,

или же HTTPS. Но в мире языка программирования Java существует не так много решений, позволяющих легко организовать зашифрованный обмен данными. В основном, имеющиеся решения либо излишне сложны, либо не обладают достаточным для серьезного использования функционалом. И именно поэтому было решено взять ранее написанную мной сетевую библиотеку, AmberNetworker, и расширить её функционал возможностью шифрования канала связи.

***Цель работы*:** разработать проект сетевой библиотеки, пригодной для использования на платформах с малым количеством доступных ресурсов (как Android-смартфоны, встраиваемые платы), а так же простой в использовании.

***Ход работы*:**

1) Проанализировать существующие библиотеки, выделить в них особенности, которые следует реализовать в своей библиотеке

2) Написать сетевую Java-библиотеку

3) Проанализировать существующие методы шифрования информации, выбрать один из них

4) Произвести брендинг, придумать логотип и написать документацию

Работа над проектом состояла из двух частей: теоретической и практической. В ходе *теоретического* исследования, я проанализировал существующие сетевые Java-библиотеки. Единственная библиотека, которая продолжает развиваться разработчиком — *Netty*. Но в ней отсутствует огромная часть нужного функционала — её создателем подразумевается то, что программист сам реализует обработку, отсылку информации. Но сама библиотека позволяет обрабатывать несколько сотен тысяч соединений одновременно и без больших потерь в производительности. Именно поэтому в основе AmberNetworker лежит библиотека Netty.

Так же в ходе теоретического исследования я рассмотрел варианты шифрования информации. Одним из простых, но в то же время мощных алгоритмов является RSA, названный так по фамилиям создателей (Rivest, Shamir, Adleman). Он работает, основываясь на модульной арифметике.

Практическая часть состояла из разработки самой библиотеки.

Она опубликована под лицензией WTFPL, которая разрешает программисту делать с исходным кодом всё, что он захочет.

Библиотека сама обрабатывает пакеты данных, следит за подключаемыми клиентами и выполняет прочие сервисные функции. Достаточно лишь зарегистрировать шаблон отправляемых данных (пакет) и создать объект библиотеки.

Затем в качестве прототипа реализации RSA шифрования была написана небольшая программа на Java, шифрующая и расшифровывающая данную строку по этому алгоритму. В ней был использован стандартный класс Java *BigInteger*, который позволять все нужные операции с большими числами — умножение, возведение в степень, возведение в степень по модулю и многое другое.

Как же работает RSA шифрование?

Представим, что у нас есть два друга — Алиса и Боб. Они хотят секретно обмениваться информацией. Пускай Алиса будет инициатором. Она придумывает два больших простых числа p и q, перемножает их и получает N — модуль. Затем она высчитывает функцию Эйлера от N — считает произведение p–1 на q–1. После этого выбирается открытый ключ e, взаимно простой с результатом функции Эйлера. И в конце считается d — закрытый ключ, который остаётся у Алисы.

$$d = e^{-1} \bmod (p-1)(q-1).$$

Далее она пересылает Бобу пару из e и N. Он шифрует своё сообщение M по формуле $C = m^e \bmod N$ и отправляет его Алисе. На данном этапе оно представляет из себя простое, «случайное» число, расшифровать которое можно только при наличии секретного ключа d. Алиса вычисляет исходное сообщение $M' = C^d \bmod N$.

На данный момент ведётся работа по внедрению этого алгоритма в код сетевой библиотеки, разработка алгоритма обмена ключами шифрования и прочими сервисными данными.

Применение библиотеки. Несмотря на своеобразность получившегося продукта, у него довольно много применений. Например, возможно внедрить её в какие-либо продукты, требующие защиты передаваемой информации, как чаты, программы для обмена документами. Так же библиотека может найти применение в образовательном секторе — данный программный продукт позволяет на практике по-

казать, как организовывается сетевой обмен данными. На данный же момент она используется в одном игровом проекте, где важна скорость обработки данных, и с чем она прекрасно справляется.

Заключение. Появление подобных IT-продуктов, положительно сказывается на имидже Калининградской области, ведь у нее есть все возможности для того, чтобы стать самой IT-продвинутой областью в стране.

В результате данного проекта создана сетевая библиотека, способная работать на самых разных устройствах, и которая позволяет шифровать передаваемые данные.

Список литературы

1. AmberNetworker / [Электронный ресурс] URL: https://bitbucket.org/uwtech/ambernetworker

2. Netty / [Электронный ресурс] URL: http://netty.io

3. RSA / [Электронный ресурс] URL: http://ru.wikipedia.org/wiki/RSA