Министерство образования и науки Российской Федерации

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ
«САРАТОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИМЕНИ Н.Г.ЧЕРНЫШЕВСКОГО»

Кафедра теоретических основ компьютерной безопасности и криптографии

Клиент Google Hangouts с криптографической защитой информации

АВТОРЕФЕРАТ

дипломной работы

студента 6 курса 631 группы
специальности 090102.65 «Компьютерная безопасность»
факультета компьютерных наук и информационных технологий
Беседина Артёма Михайловича

Научный руководитель
доцент, к.ф.-м.н. А.В. Жаркова

Заведующий кафедрой
профессор, к.ф.-м.н. В.Н. Салий

Саратов 2016

ВВЕДЕНИЕ

Без использования криптографии сегодня немыслимо решение задач по обеспечению безопасности информации. Если до 1990 года криптография обеспечивала закрытие исключительно государственных линий связи, то в наши дни использование криптографических методов получило широкое распространение благодаря развитию компьютерных сетей и электронного обмена данными в различных областях: финансах, банковском деле, торговле и т.п. [1] Огромное распространение в наше время получила всемирная система объединенных компьютерных сетей – Интернет. Интернет – это средство для получения доступа к самой разнообразной информации, а также средство общения, по эффективности и популярности не уступающее телефону. В связи с этим встает угроза целостности и конфиденциальности той информации, которую вы доверяете Интернет. Использование криптографических методов для защиты этой информации является одним из способов предотвращения таких угроз.

Существует огромное количество веб-сервисов и программ, предназначенных для обмена информацией через Интернет. Число пользователей некоторых из них достигает несколько сотен миллионов человек. Например, по последним данным сервисами Google, доступ к которым осуществляется через один Google аккаунт, пользуются 425 миллионов человек по всему миру. Одним из таких сервисов является Hangouts (ранее Google Talk), который позволяет обменивается мгновенными сообщениями с другими владельцами Google аккаунтов. В связи с такой распространенностью систем мгновенного обмена сообщениями, возникает необходимость сохранения конфиденциальности переписки. Шифрование сообщений – один из способов решения этой проблемы.

Целью данной дипломной работы является рассмотрение некоторых существующих программ мгновенного обмена сообщениями, предлагающих

шифрование соответствующей информации, изучение алгоритмов и стандартов, с помощью которых можно организовать криптографическую защиту передаваемой информации, в результате чего требуется разработать и реализовать Hangouts клиент мгновенного обмена сообщениями с криптографической защитой информации.

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

Данная дипломная работа начинается с введения, где поднимается вопрос безопасности информации, передаваемой через интернет, и ставится цель данной дипломной работы.

Первый раздел «Необходимые понятия и алгоритмы» посвящен рассмотрению необходимых понятий, определений, алгоритмов и протоколов. В подразделе 1.1 «Необходимые определения» приведены основные определения, которые встречаются в работе. Подраздел 1.2 «Блочные шифры» даёт общее представление о блочных шифрах, принципе их построения и режимах работы, в том числе описывается стандарт шифрования Российской Федерации ГОСТ 28147-89. Подраздел 1.3 «Распределения ключей» поднимает проблему распределения ключей и приводит описание нескольких протоколов, в том числе рассматривается протокол открытого распределения ключей Диффи-Хеллмана.

Во втором разделе «Некоторые существующие программные продукты, реализующие шифрование сообщений» рассматриваются некоторые программные продукты, реализующие шифрование сообщение, такие как Telegram, Pidgin, Silent Phone, SJ Messenger, Wickr, Cryptocat.

Третий раздел «Разработка программного продукта» посвящен разработанному и реализованному автором программному продукту. Программа представляет собой клиент для Hangouts с криптографической защитой передаваемой информации, построенный с использованием стандарта шифрования Российской Федерации ГОСТ 28147-89 и алгоритма распределения ключей Диффи-Хеллмана. Подраздел 3.1 «Реализация» описывает реализацию данного программного продукта и принцип его работы. Подраздел 3.2 «Использование программы» представляет собой подробное описание использования программы, сопровождающееся соответствующими снимками экрана.

Завершается данная дипломная работа заключением, списком использованных источников и приложением «А», в котором приведен листинг программы.

ЗАКЛЮЧЕНИЕ

В ходе данной работы были рассмотрены блочные шифры, их спецификации и принципы работы, в том числе был изучен стандарт шифрования Российской Федерации ГОСТ 28147-89, рассмотрены протоколы распределения ключей, в том числе алгоритм открытого распределения ключей Диффи-Хеллмана. Также был проведено изучение некоторых существующие программных продуктов, реализующих шифрование сообщений, их возможности, используемые протоколы и алгоритмы защиты.

В результате проделанной работы была разработана и реализована программа-клиент для Hangouts с криптографической защитой передаваемой информации на основе стандарта шифрования Российской Федерации ГОСТ 28147-89 и алгоритма распределения ключей Диффи-Хеллмана.

Таким образом, все поставленные задачи были полностью решены.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1 Основы криптографии / А. П. Алферов, А. Ю. Зубов, А. С. Кузьмин, А. В. Черемушкин. М. : Гелиос АРФ, 2002. 480 с.

2 Салий, В. Н. Криптографические методы и средства защиты информации: учеб. пособие / В. Н. Салий // СГУ – Саратовский государственный университет [Электронный ресурс] : [сайт]. URL: www.sgu.ru/sites/default/files/textdocsfiles/2015/11/09/saliy_v.n._kriptograficheskie_metody_i_sredstva_zashchity_informacii.pdf (дата обращения: 15.12.2015). Загл. с экрана. Яз. рус.

3 Криптографическая стойкость [Электронный ресурс] // Википедия [Электронный ресурс] : свободная энциклопедия. URL: ru.wikipedia.org/wiki/Криптографическая_стойкость (дата обращения: 15.12.2015). Загл. с экрана. Яз. рус.

4 Сервер (программное обеспечение) [Электронный ресурс] // Википедия [Электронный ресурс] : свободная энциклопедия. URL: ru.wikipedia.org/wiki/Сервер_(программное_обеспечение) (дата обращения: 15.12.2015). Загл. с экрана. Яз. рус.

5 Клиент (информатика) [Электронный ресурс] // Википедия [Электронный ресурс] : свободная энциклопедия. URL: ru.wikipedia.org/wiki/Клиент_(информатика) (дата обращения: 15.12.2015). Загл. с экрана. Яз. рус.

6 Система мгновенного обмена сообщениями [Электронный ресурс] // Википедия [Электронный ресурс] : свободная энциклопедия. URL: ru.wikipedia.org/wiki/Система_мгновенного_обмена_сообщениями (дата обращения: 15.12.2015). Загл. с экрана. Яз. рус.

7 Первообразный корень (теория чисел) [Электронный ресурс] // Википедия [Электронный ресурс] : свободная энциклопедия. URL:

ru.wikipedia.org/wiki/Первообразный_корень_(теория_чисел) (дата обращения: 15.12.2015). Загл. с экрана. Яз. рус.

8 Введение в криптографию с открытым ключом [Электронный ресурс] // «ИНТУИТ» Национальный открытый университет [Электронный ресурс]. URL: www.intuit.ru/studies/courses/691/547/lecture/12387 (дата обращения: 15.12.2015). Загл. с экрана. Яз. рус.

9 Функция Эйлера [Электронный ресурс] // Википедия [Электронный ресурс] : свободная энциклопедия. URL: ru.wikipedia.org/wiki/Функция_Эйлера (дата обращения: 15.12.2015). Загл. с экрана. Яз. рус.

10 Шнайер, Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си / Б. Шнайер. М. : Издательство ТРИУМФ, 2003. 816 с.

11 Блочные шифры [Электронный ресурс] // Криптография [Электронный ресурс]. URL: kryptography.narod.ru/block.html (дата обращения: 15.12.2015). Загл. с экрана. Яз. рус.

12 Блочные шифры и их криптоанализ [Электронный ресурс] // Энциклопедия теоретической и прикладной криптографии [Электронный ресурс] : свободная энциклопедия. URL: cryptowiki.net/index.php?title=Блочные_шифры_и_их_криптоанализ (дата обращения: 15.12.2015). Загл. с экрана. Яз. рус.

13 Симметричные системы и блочные шифры [Электронный ресурс] // Дискретная математика: алгоритмы [Электронный ресурс]. URL: rain.ifmo.ru/cat/view.php/theory/coding/cryptography-2005/block (дата обращения: 15.12.2015). Загл. с экрана. Яз. рус.

14 О введении новых криптографических стандартов, разработанных с участием ИнфоТеКС [Электронный ресурс] // Infotecs [Электронный ресурс]. URL: infotecs.ru/press/news/15/14508/ (дата обращения: 15.12.2015). Загл. с экрана. Яз. рус.

15 ГОСТ 28147-89 [Электронный ресурс] // Википедия [Электронный ресурс] : свободная энциклопедия. URL: ru.wikipedia.org/wiki/ГОСТ_28147-89 (дата обращения: 15.12.2015). Загл. с экрана. Яз. рус.

16 ГОСТ Р 34.13–2015 «Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров» // Технический комитет по стандартизации «Криптографическая защита информации» (ТК 26) [Электронный ресурс] : [сайт]. URL: www.tc26.ru/standard/gost/GOST_R_3412-2015.pdf (дата обращения: 15.12.2015). Загл. с экрана. Яз. рус.

17 Проблема распределения ключей. Криптосистема с общим ключом. Концепции односторонней функции. Частный секретный ключ. [Электронный ресурс] // Сайт специальности "Организация и Технология Защиты Информации" (ОиТЗИ) Самарского Государственного Экономического Университета [Электронный ресурс]. URL: oitzi.ru/Materials.aspx?doc_id=31&id=677 (дата обращения: 15.12.2015). Загл. с экрана. Яз. рус.

18 Открытое распределение ключей [Электронный ресурс] // Энциклопедия теоретической и прикладной криптографии [Электронный ресурс] : свободная энциклопедия. URL: cryptowiki.net/index.php?title=Блочные_шифры_и_их_криптоанализ (дата обращения: 15.12.2015). Загл. с экрана. Яз. рус.

19 Протокол Диффи-Хеллмана [Электронный ресурс] // Википедия [Электронный ресурс] : свободная энциклопедия. URL: cryptowiki.net/index.php?title=Открытое_распределение_ключей (дата обращения: 15.12.2015). Загл. с экрана. Яз. рус.

20 Обзор зашифрованных мессенджеров для IOS [Электронный ресурс] // Hi-tech вести [Электронный ресурс]. URL: http://hitech.vesti.ru/news/view/id/3328 (дата обращения: 15.12.2015). Загл. с экрана. Яз. рус.

21 Встречайте, Телеграм: Защищенный мессенджер на базе MTProto. // Telegram [Электронный ресурс]. URL: https://tlgrm.ru (дата обращения: 15.12.2015). Загл. с экрана. Яз. рус.

22 Новая версия российского Telegram для iOS и Android [Электронный ресурс] // Hi-tech вести [Электронный ресурс]. URL: http://ru.appmess.com/news/updates/26136-obnovleniya-telegram-dlya-ios-i-android-video-i-poisk-v-chatax/ (дата обращения: 15.12.2015). Загл. с экрана. Яз. рус.

23 Мобильный протокол MTProto [Электронный ресурс] // Telegram [Электронный ресурс]. URL: https://tlgrm.ru/docs/mtproto (дата обращения: 15.12.2015). Загл. с экрана. Яз. рус.

24 Безопасный интернет-мессенджер [Электронный ресурс] // Kaspersky lab daily [Электронный ресурс]. URL: https://blog.kaspersky.ru/cryptomessaging/3691/ (дата обращения: 15.12.2015). Загл. с экрана. Яз. рус.

25 Pidgin // Pidgin [Электронный ресурс]. URL: pidgin.im (дата обращения: 15.12.2015). Загл. с экрана. Яз. рус.

26 Pidgin + OTR [Электронный ресурс] // Security in-a-box [Электронный ресурс]. URL: https://securityinabox.org/ru/pidgin_main (дата обращения: 15.12.2015). Загл. с экрана. Яз. рус.

27 Off-the-Record Messaging [Электронный ресурс] // Википедия [Электронный ресурс]: свободная энциклопедия. URL: http://ru.wikipedia.org/wiki/Off-the-Record_Messaging (дата обращения: 15.12.2015). Загл. с экрана. Яз. рус.

28 Silent circle [Электронный ресурс] // Silent Circle [Электронный ресурс]. URL: www.silentcircle.com (дата обращения: 15.12.2015). Загл. с экрана. Яз. рус.

29 Answers to your ZRTP Questions [Электронный ресурс] // Silent Circle [Электронный ресурс]. URL: www.silentcircle.com/products-and-

solutions/technology/zrtp/?q=aes+#what-is-zrtp (дата обращения: 15.12.2015). Загл. с экрана. Яз. рус.

30 SJ IM Messenger [Электронный ресурс] // SJ Software [Электронный ресурс]. URL: ios.safetyjabber.com/index.html (дата обращения: 15.12.2015). Загл. с экрана. Яз. рус.

31 PGP [Электронный ресурс] // Википедия [Электронный ресурс]: свободная энциклопедия. URL: http://ru.wikipedia.org/wiki/OpenPGP (дата обращения: 15.12.2015). Загл. с экрана. Яз. рус.

32 The Most Trusted Messenger in the World [Электронный ресурс] // Wickr [Электронный ресурс]. URL: www.wickr.com (дата обращения: 15.12.2015). Загл. с экрана. Яз. рус.

33 Мессенджеры для параноиков [Электронный ресурс] // Tjournal [Электронный ресурс]. URL: http://tjournal.ru/paper/paranoid-messengers (дата обращения: 15.12.2015). Загл. с экрана. Яз. рус.

34 Обзор приложения: Wickr – самый секретный мессенджер [Электронный ресурс] // Androidpit [Электронный ресурс]. URL: http://www.androidpit.ru/wickr-secret (дата обращения: 15.12.2015). Загл. с экрана. Яз. рус.