С.Сейфуллиннің 125 жылдығына арналған **«Сейфуллин оқулары – 15: Жастар, ғылым, технологиялар: жаңа идеялар мен перспективалар»** атты халықаралық ғылыми-теориялық конференциясының материалдары = Материалы Международной научно-теоретической конференции **«Сейфуллинские чтения – 15: Молодежь, наука, технологии – новые идеи и перспективы»**, приуроченной к 125-летию С.Сейфуллина. - 2019. - Т.II, Ч 1 - С.165-166

О КРИПТОГРАФИЧЕСКОЙ СТОЙКОСТИ И КИБЕРБЕЗОПАСНОСТИ

Шекеров Н.Т.

Криптографическая стойкость (или криптостойкость) — способность криптографического алгоритма противостоять криптоанализу. Стойким считается алгоритм, атака на который требует от атакующего наличия столь значительных вычислительных ресурсов или огромных затрат времени на расшифровку перехваченных сообщений, что к моменту их расшифровки защищённая информация потеряет свою актуальность. Вот и лист кибератак в реальном времени по версий Лаборатории Касперского [1-2]. (Рисунок 1):

Рисунок 1 – Количество обнаружений кибератак в секунду по всему миру

OAS - 3.5 M/S (On-Access Scan) - автоматическая проверка. Показывает поток данных по вредоносным программам, обнаруженным во время открытия, копирования, запуска или сохранения файлов.

ODS – 2.1M/S (On Demand Scanner)- Проверка по требованию показывает поток данных по вредоносным программам, возникающий, когда пользователь вручную выбирает "Просканировать компьютер" в меню.

MAV – 0.1 M/S (Mail Anti-Virus)- Почтовый антивирус показывает поток данных по вредоносным программам, обнаруженным среди новых объектов в почтовых приложениях. Почтовый антивирус проверяет входящие сообщения и запускает автоматическую проверку при сохранении вложенных файлов на диск.

WAV- 1M/S (Web Anti-Virus)- Веб-антивирус показывает поток данных по вредоносным программам, обнаруженным при открытии HTML-страниц веб-сайтов, а также при загрузке файлов. Веб-антивирус проверяет порты, указанные в его настройках

.IDS - 1.7M/S (Intrusion Detection Scan)- Система обнаружения вторжений показывает поток данных по обнаруженным сетевым атакам.

VUL- 60 000/S (Vulnerability Scan)- Поиск уязвимостей показывает поток данных по обнаруженным уязвимостям.

KAS – 3.4 M/S(Kaspersky Anti-Spam) - Касперский Анти-Спам показывает подозрительный и нежелательный почтовый трафик, обнаруженный с помощью технологий репутационной фильтрации «Лаборатории Касперского».

BAD – 343/S(Botnet Activity Detection) - Мониторинг активности ботнетов показывает статистику по выявленным IP-адресам жертв DDoS-атак и IP-адресам командных серверов ботнетов. Статистика собирается с помощью системы DDoS Intelligence, входящей в состав решения Kaspersky DDoS Prevention.

А на предыдущий месяц лидером по уязвимости занял Таджикистан 42% всех компьютеров страны заражен вирусами, а Казахстан занял 17 место.

Напомню, что сейчас все соц. сети и большие коммерческие сайты и электронные банки используют относительно безопасные шифрование по протоколу RSA разной длиной ключа (например для Google это равна 1024 бит до 2010 года, различные банки государственного уровня используют 2048 бит).

До 2009 года RSA 1024 считалась самой безопасной, но только на ближайшие 2-4 года, так же в этом году группе учёных из Швейцарии, Японии, Франции, Нидерландов, Германии и США удалось успешно рассчитать данные, зашифрованные при помощи криптографического ключа стандарта RSA длиной 768 бит.[3].

В своем примере использование протокола RSA смог создать наиболее безопасное средство для обмена путем использование 2048 битного шифрование, так же реализовал систему защиту от атак, а так же динамическую генераций ключа.

Как работает это система? Программа на стадии бета теста. Вы шифруете с помощью ключа данные и система отправляет конечный ключ и зашифрованное послание на вашу электронную почту. Есть 2 программа для расшифровки если второй пользователь вводит 3 раза неправильно ключ, то программа посчитает это как потенциальный взлом и заново сгенерирует ключ и отправит на вашу почту, таким образом старый ключ станет не актуальным (пример на 2 рисунке).

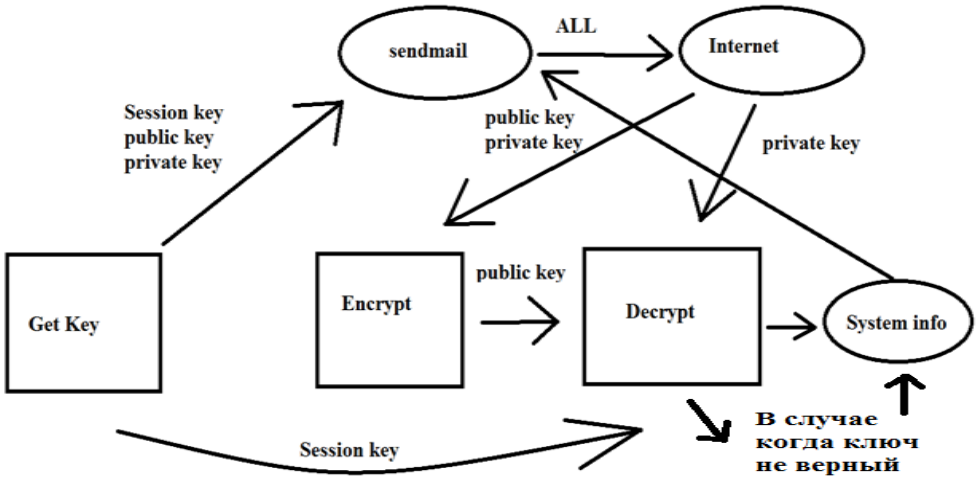

Рисунок 2. Пример работы программы

Список литературы

1. McBride L,E., Jr. and K.S.Narendra. The five pillars of cybersecurity readiness // IEM Information Security, 2017.vol 47, p.131-145

2. https://ru.wikipedia.org/wiki/Криптрографическая_Стойкость

3. https://cybermap.kaspersky.com/ru/stats/#country=39&type=oas&period=m

4. https://ru.wikipedia.org/wiki/криптоанализ

Научный руководитель: Старший преподаватель кафедры «Вычислительная техника и программное обеспечения» Калдарова М.Ж