ИСЛЕДОВАНИЕ АКТУАЛЬННЫХ АЛГОРИТМОВ ШИФРОВАНИЯ, ПРИМЕНЯЕМЫХ НА СОВРЕМЕННЫХ МОБИЛЬНЫХ УСТРОЙСТВАХ ПОД УПРАВЛЕНИЕМ ОПЕРАЦИОННОЙ СИСТЕМОЙ ANDROID

Якимович А.В., Прохоренко А.С.
Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь
Ионин В.С – канд.техн.наук, доцент

Цель работы – рассмотрение и анализ актуальных алгоритмов шифрования, применяемых на современных мобильных устройствах под управлением операционной системы Android.

Для защиты и безопасности данных на цифровых устройствах используется множество алгоритмов шифрования. С помощью шифрования обеспечиваются три состояния безопасности информации: конфиденциальность, целостность и идентифицируемость. Существующие алгоритмы шифрования могут применяться в различных ситуациях, обеспечивать различные методы шифрования, а также включать различные уровни производительности.

На данный момент в мире среди всех устройств люди используют в большей степени мобильные устройства [1]. Так же сейчас преобладающее большинство мобильных устройств используют операционную систему *Android* [2]. Так что среди всех цифровых устройств наибольшей группой устройств являются мобильные устройства под управлением операционной системы Android. Что и вызывает большой интерес из-за большой сферы влияния защиты данных на данную группу устройств.

Столь большая группа цифровых устройств находится в довольно неудобном положении из-за того, что располагает небольшим количеством вычислительных ресурсов по сравнению с стационарными устройствами. Важной задачей является поиск баланса между безопасностью данных и производительностью.

Рассматривается так же возможные угрозы [3] и необходимость перехода со старых и не безопасных алгоритмов шифрования таких как например *SHA-1* [4] на актуальные отвечающие современным стандартам безопасности алгоритмы шифрования SHA-2 [5]. На рисунке 1 приведена схема одной итерации алгоритмов SHA-2/

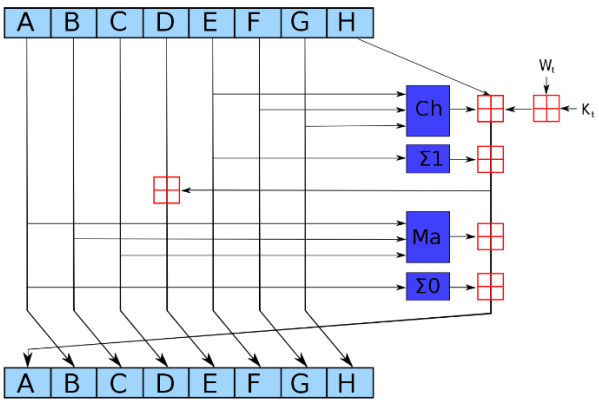

Рисунок 1 – Схема одной итерации алгоритмов SHA-2

В результате можно сделать вывод, что современные мобильные устройства нуждаются в надёжном и эффективном способе шифрования, который не будет затрачивать большие ресурсы устройства.

Список использованных источников:

1. Данные распределения типов цифровых устройств [Электронный ресурс]. – Режим доступа: https://gs.statcounter.com/platform-market-share/desktop-mobile-tablet/worldwide/2019. – Дата доступа: 25.03.2020.

2. Данные распределения операционных систем среди устройств [Электронный ресурс]. – Режим доступа: https://gs.statcounter.com/os-market-share. – Дата доступа: 25.03.2020.

3. Взлом криптографического хеширования SHA-1 [Электронный ресурс]. – Режим доступа: https://www.schneier.com/blog/archives/2005/02/sha1_broken.html. – Дата доступа: 25.03.2020.

4. Алгоритм криптографического хеширования SHA-1 [Электронный ресурс]. – Режим доступа: https://tools.ietf.org/html/rfc3174. – Дата доступа: 25.03.2020.

5. Алгоритм криптографического хеширования SHA-2 [Электронный ресурс]. – Режим доступа: https://tools.ietf.org/html/rfc3874. – Дата доступа: 25.03.2020.