КРИПТОУСТОЙЧИВОСТЬ ПРИ КОДИРОВАНИИ ИНФОРМАЦИИ НА МОБИЛЬНЫХ УСТРОЙСТВАХ

Шинкарук В.В.

Республиканское высшее учебное заведение
«Крымский гуманитарный университет»,
г. Ялта

В настоящее время существует большое количество разнообразных криптографических алгоритмов [1, 2], однако высокие вычислительные требования к устройствам – малый объём памяти, низкая частота процессора, малая лояльность к многозадачным приложениям [3] – зачастую являются определяющими фактором в выборе того или иного криптографического алгоритма для реализации его на мобильных платформах. Таким образом, упрощение вычислительной реализации алгоритмов кодирования информации на мобильных устройствах становится здесь задачей, которая по своей сложности соизмерима с проблемой повышения криптостойкости этих алгоритмов.

В работе представлена разработка простой для реализации на мобильном устройстве схемы кодирования информации. За основу взята схема кодирования с закрытым ключом.

Важно понимать, что данная схема предназначена именно для кодирования информации, хранящейся на устройстве, поэтому при построении соответствующих алгоритмов упор делается на как можно более существенную зависимость выходных данных от ключа и исходного сообщения; однако это ещё не означает, что нужно создавать сложные и трудно вычислимые функции.

Для программной реализации желательно выбрать язык Java, как наиболее подходящий для быстрого написания эффективных приложений, в том числе и приложений работающих с изолированной памятью.

В результате проведенных исследований, должен получиться вариант схемы кодирования информации на мобильном устройстве и построен простой алгоритм, реализующий подобную схему. При этом нужно отметить, что шифрование текстовой информации является лишь одним из примеров применения описанной схемы кодирования – можно так же успешно разработать приложение для шифрования файлов, записанных на мобильном устройстве.

Литература:

1. Горбатов В.А. Дискретная математика/ Горбатов В.А., Горбатов А.В, Горбатова М.В. – М.: АСТ Астрель, 2006.

2. Новиков Ф.А. Дискретная математика для программистов/ Ф.А. Новиков. – СПб: Питер, 2002.

3. Горнаков С.Г. Программирование мобильных телефонов на Java 2 Micro Edition / С.Г. Горнаков. – М.: ДМК Пресс, 2004.