ИССЛЕДОВАНИЕ ВЛИЯНИЯ ДЛИТЕЛЬНОСТИ ХЕШ-ФУНКЦИИ И ИЗМЕНЕНИЯ ВЕРОЯТНОСТИ КОЛЛИЗИЙ НА УСТОЙЧИВОСТЬ КРИПТОГРАФИЧЕСКОЙ ХЕШ-ФУНКЦИИ К АТАКАМ

А.М. Макаров, Е.А. Писаренко, А.С. Ермаков, Д.А. Паринова

Одной из важных характеристик, влияющих на стойкость к атакам путем перебора возможных текстов, является длина хеш-функции. В работах [1–3] были рассмотрены атаки на основе парадокса дня рождения и «встречи посередине» применительно к хеш-функции, построенной по схеме Рабина. В приведенных исследованиях были получены результаты для больших значений длины хэш-функции.

При использовании технологий криптографии в системах, имеющих практический интерес для социально-экономической сферы, желательно получить точные оценки влияния параметра, связанного с длинной хэш-функции, на стойкость ее к атакам типа «атака в лоб». Таким параметром служит число переборов, зависящее от вероятности коллизий и длины хеш-функции.

В результате проведенного исследования было получено точное выражение для нахождения числа переборов и определено влияние длины хеш-функции и изменения вероятности коллизии на устойчивость криптографической хеш-функции.

Расчеты числа переборов, проведенные с помощью выведенной формулы, позволили визуализировать зависимость их от длины хеш-функции при заданной вероятности коллизии $P = 0{,}5$. Кроме того, были получены формы графиков при отклонении вероятности коллизии от 0,5 ка в одну, так и в другую сторону.

Полученные результаты точного анализа характеристик криптостойкости хэш-функций в зависимости от ее длинны позволяют найти компромисс между стойкостью ее к атакам, быстродействием обработки данных и затратами на аппаратуру.

Литература

1. Молдовян Н.А., Молдовян А.А. Введение в криптосистемы с открытым ключом. СПб.: БХВ-Петербург, 2005. 228 с.

2. Мао В. Современная криптография: теория и практика. М.: Издательский дом «Вильямс», 2005. 768 с.

3. Haber S., Stornetta W.S. How to Time-Stamp a Digital Document // J. Cryptology. 1991. P. 99–111.