УДК 512.624.95:378.147.091.3

Односторонние функции в защите информации

Крупенкова Т.Г., Липницкий В.А.
Белорусский национальный технический университет,
Военная академия Республики Беларусь

Мы живём в эпоху, которую принято называть информационной. Это означает глубокое слияние мира реального и виртуального – мира телекоммутационных и информационных сетей. Как никогда актуальной стала проблема защиты информации – обеспечение её надёжности, достовености, точности, защита её от помех и вмешательств от несанкционированного доступа.

Практически всегда возникающие перед человечеством проблемы проходят предварительную аппробацию в умах интеллектуальной элиты. Так и здесь – основные проблемы современной защиты информации были озвучены примерно 40 лет тому назад в 1976 году Уитфилдом Диффи и Мартином Хелманом. Один из трёх высказанных ими тезисов заключается в необходимости применения для защиты информации идеи об односторонних функциях. Внешне по своей сути простая, эта идея на самом деле несёт в себе глубочайший научный, философский и практический смысл.

Односторонней называется однозначная обратимая функция, значения которой достаточно легко вычисляются, но значения обратной функции практически невозможно найти без дополнительной информации.

В любом надёжном алгоритме шифрования должна быть заложена односторонняя функция. Действительно, одни из самых популярных криптосистем – криптосистемы RSA и Рабина базируются на сложности решения задачи, обратной к вычислению произведения двух больших чисел. Столь же популярная криптосистема Эль Гамаля базируется на проблеме дискретного логарифмирования.

На сегодняшний день строго математически не доказано, что упомянутые выше примеры действительно относятся к разряду односторонних функций. Ведутся интенсивные исследования по разработке полиномиальных алгоритмов решения названных задач. Но результаты пока отрицательные. Попытки найти иные примеры односторонних функций остаются безуспешными. XTR криптосистема, ECC-криптография базируются на различных модификациях задачи дискретного логарифмирования.

Односторонние функции можно представить, как взгляд сверху на проблему современной криптографии, позволяющий классифицировать любые криптографические системы, оценить их достоинства и недостатки.