УДК 004.056.55

ОЦЕНКА КРИПТОСТОЙКОСТИ МЕТОДА ОБЪЕДИНЕНИЯ НЕСКОЛЬКИХ СООБЩЕНИЙ В ОДНОМ ШИФРТЕКСТЕ

Голованов А. А. (Университет ИТМО), **Иогансон И. Д.** (Университет ИТМО),
Дакуо Ж.-М. Н. (Университет ИТМО)
Научный руководитель – д. т. н., доцент Беззатеев С. В.
(Университет ИТМО)

В данной работе проводится оценка криптостойкости криптографического метода объединения сообщений нескольких пользователей в одном шифртексте.

Введение. Существует концепция криптографических схем, которые из одного шифртекста получить разные открытые тексты в зависимости от ключа, используемого в операции дешифрования. Задача состоит в разработке подобной криптографической схемы.

Основная часть. В ходе работы созданы два прототипа описанной криптографической схемы: на основе китайской теоремы об остатках и на основе ортогональных линейных кодов.

Первая схема использует китайскую теорему об остатках, чтобы установить биекцию между вектором открытых текстов и шифртекстом: открытое сообщение получается из шифртекста путём нахождения остатка от деления шифртекста на целочисленное выражение ключа. Получение шифртекста из открытых текстов выполняется по алгоритму китайской теоремы об остатках. Расширение схемы – введение дополнительного случайного открытого текста для обеспечения вероятностной составляющей. Данная схема является переосмыслением схемы разделения секрета М. Миньотта.

Вторая схема основана на свойствах ортогональных линейных кодов. Порождающие матрицы этих кодов в схеме являются ключами. Шифртекст является суммой кодовых слов, полученных из сообщений, выраженных в виде информационных векторов. Путём специального преобразования порождающей матрицы пользователь получает матрицу, при умножении на которую шифртекст преобразуется в исходное сообщение, соответствующее ключу.

В данной работе проводится оценка безопасности для данных прототипов. В частности, с помощью методов теории вычислительной сложности проводится оценка сложности нахождения ключей пользователей при известном ключе одного из пользователей, а также при отсутствии такой информации.

Выводы. Проведена оценка сложности спроектированных криптосхем, объединяющих несколько открытых текстов в одном шифртексте. Проведённая оценка будет использована для создания безопасной криптосхемы такого рода.

Криптографический метод объединения сообщений нескольких пользователей в одном шифртексте имеет потенциал для приложений: системы «вход под принуждением», организация доступа в секретные архивы, создание карт лояльности нескольких компаний.

Голованов А. А. (автор) Подпись

Беззатеев С. В. (научный руководитель) Подпись