УДК 004.056

Розломій І.О., канд. техн. наук
Науменко С.В.
Черкаський національний університет ім. Б. Хмельницького, inna-roz@ukr.net

МЕТОДОЛОГІЯ ВИКОРИСТАННЯ МАТРИЧНИХ РЕШІТОК КАРДАНО ДЛЯ КОМПЛЕКСНИХ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ

В даний час майже всі дані переходять в електронний вигляд. Разом з переходом інформації в цифрове середовище вдосконалюються методи несанкціонованого доступу до неї. Тому зараз, галуззю, яка стрімко розвивається, стає розробка та вдосконалення механізмів та засобів забезпечення безпеки даних. В зв'язку із зростанням кількості способів нелегального проникнення до інформації, засоби захисту інформації не повинні обмежуватися лише апаратними чи програмними. Захист інформації – це комплекс заходів, спрямованих на забезпечення інформаційної безпеки. Для забезпечення захисту інформації використовуються інструменти криптографії, стиснення та прихованої передачі даних.

Пропонується методологія використання матричних решіток для вирішення задач захисту інформації. Типова решітка Кардано, яку ще називають шифрувальною решіткою представляє собою трафарет прямокутної чи квадратної форми з отворами. В отвори записують інформацію, яку необхідно зашифрувати. Існує багато модифікацій решітки Кардано, зокрема поворотна решітка [1]. Прототип стандартної решітки Кардано був взятий за основу для створення матричної решітки. Матричні решітки Кардано побудовані на основі статистичного аналізу художнього англомовного тексту та виконання операцій матричного криптографічного перетворення інформації [2]. Решітка заповнюється літерами англійського алфавіту. Спочатку необхідно виконати частотний аналіз тексту, на основі якого визначити частоту входження кожної літери в решітку. Операції матричного криптографічного перетворення вкажуть на розміщення літер в комірках решітки. Розроблена матрична решітка Кардано придатна для вирішення задач захисту текстової інформації.

Розглянемо детальніше принципи використання матричної решітки Кардано для шифрування, стиснення та прихованої передачі інформації.

Шифрування інформації матричною решіткою полягає в отриманні послідовності чисел, які вказують на комірки решітки, в котрих міститься інформація, яку необхідно зашифрувати в решітці. Звідси і схожість матричної решітки з типовою шифрувальною решіткою Кардано.

Стиснення інформації – алгоритмічне перетворення даних, яке виконується з метою зменшення їх обсягу. Оскільки для всіх художніх текстів характерною є надлишковість, доречним є їх стиснення. Стиснення інформації за допомогою матричної решітки Кардано передбачає процес заміни повторюваних символів парою чисел – зміщення і кількість повторюваних символів.

На останок, прихована передачі інформації відкритими каналами зв'язку передбачає приховування самого факту передачі інформації, так як, передається не сама інформація, а лише пара чисел.

Подальший розвиток дослідження передбачає пошук матриці, яка стискає тексти якомога більшого розміру для визначення авторства.

Список посилань

1. Грицюк Ю.І., Грицюк П.Ю. Математичні основи процесу генерування ключів переставлення з використанням шифру Кардано / Ю.І. Грицюк, П.Ю. Грицюк // Науковий вісник НЛТУ. – 2015. – №10(25). – С. 311–323.

2. Розломій І.О. Метод побудови матричних решіток Кардано для стиснення інформації / І.О. Розломій // Вісник ХНУ. Технічні науки. 2022. – №1(305). – С. 85–90.