УДК 621.391

ШИФРУВАННЯ ДАНИХ З ВИКОРИСТАННЯМ МАТРИЦЬ

Бобко О. Л.
Науковий керівник – доц., к.т.н. Майданюк В. П.

Головним завданням будь-якого алгоритму шифрування є ефективне перемішування та розсіювання даних. Для цього використовують шифри перестановки. Один з підходів до виконання перестановок полягає у застосуванні матричних перетворень. Перестановки виконуються над двовимірними блоками даних розміром nxn за рахунок використання операцій над матрицями. Зокрема таких як транспонування матриць, операції з масками. Довжини слів, що перемішуються, можуть змінюватися для кожного блоку від 1 до m біт псевдовипадковим чином, що значно ускладнює криптоаналіз зашифрованого тексту. Для реалізації даного підходу використовуються дві матриці – матриця-ключа і матриця даних, що мають однакову розмірність nxn, причому обов'язково щоб n було парним числом. Кожен елемент матриці-ключа може містити одиницю або нуль, що задає порядок заповнений матриці даних. Наприклад, матриця-ключ може бути поділена на чотири частини, три з яких заповнюються одиницями, а четверта – нулями.

Припустимо необхідно перемішати блок даних розміром nxn. Матриця-ключ накладається на матрицю даних, після чого відбувається наступне: послідовно розглядається кожен і-й елемент матриці-ключа. Якщо і-й елемент має значення «0», то у відповідний і-й елемент матриці даних записується наступний символ з послідовності, яку необхідно зашифрувати. Коли перегляд добігає кінця, матриця-ключ транспонується, що відкриває нові елементів, які можна заповнити. Після чотирьох ітерацій, матриця даних повністю буде заповнена символами. Потім необхідно зчитати символи, що і формує перемішану послідовність на виході. Заключним етапом є шифрування проміжного шифру методом гамування шляхом накладення гами шифру з виходу генератора псевдовипадкових чисел на дані проміжного шифру з використанням операції виключного «АБО». Особливість операції виключного «АБО» полягає в тому, що якщо до значення елемента даних додати ключ, а потім до результату знову додати ключ, то отримаємо початкове значення.

Дешифрування виконуються з використанням аналогічних операцій, тобто алгоритм симетричний. Для реалізації даного методу розроблена програма мовою Java SE, завдяки чому вона є кросплатформенною, що дозволяє використовувати її для шифрування даних не тільки на комп'ютерах, але і інших пристроях, зокрема мобільних, які підтримують Java. В програмі використовуються матриці ключа і даних розміром 10x10. Елементи матриці даних можуть мати довжини від одного до восьми біт. Дослідження розподілу частот символів після шифрування показали, що він близький до рівномірного, що свідчить про достатньо високу криптостійкість алгоритму шифрування.