**УДК 681.3.001.63**

**ГЕНЕТИЧНИЙ АЛГОРИТМ В КРИПТОАНАЛІЗІ**

*Лавренюк Ю.Ю.*

**Гриник Р.О.**, викладач, кафедра УІБ

Львівський державний університет безпеки життєдіяльності

Шифрування інформації в теперішній час стало чи не основним методом її захисту. Доступність обчислювальної техніки та стрімкий прогрес в її розвитку привели до вдосконалення давно відомих шифрів і застосування в масовому масштабі нових високонадійних схем шифрування. Однак і в цьому прогресі є інша сторона: всі ці можливості обчислювальних пристроїв сьогодні успішно використовуються не тільки для шифрування, але й для «злому» тих шифрів, які ще вчора, здавалося, гарантували повний захист інформації.

Одним з нових алгоритмів, які використовуються з метою злому шифрів виступає генетичний алгоритм. В основі цього алгоритму лежить використання механізмів, що нагадують механізми природної еволюції для знаходження мінімуму (максиму) заданої функції [1]. Генетичний алгоритм вирішує задачу криптографічного аналізу в два етапи. На першому етапі він знаходить довжину секретного ключа, а на другому – сам ключ.

Розглянемо тепер задачу знаходження довжини ключа за наявним зашифрованим текстом. Нехай N - передбачуване значення довжини справжнього секретного ключа, а L - його справжня довжина. Якщо числа N і L збігаються, то можна очікувати, що знайдена в результаті роботи генетичного алгоритму перестановка буде близька до шуканої, а цільова функція при використанні цієї перестановки набуде відносно невеликого значення.

Відзначимо, що для прискорення роботи алгоритму при знаходженні довжини ключа можна використовувати малі чисельності популяції і невелике число поколінь, а після знаходження істинної довжини ключа L можна повторно застосувати генетичний алгоритм з великими значеннями параметрів для відшукання самого секретного ключа [3].

Застосування генетичного алгоритму не гарантує повного дешифрування, але зазвичай отриманий на виході текст мало відрізняється від оригіналу. Як правило, при правильному підборі параметрів мутації та схрещування генів, даний алгоритм показує досить хороші результати.

**ЛІТЕРАТУРА**

1. Алфьоров А.П., Зубов А.Ю., Кузьмін А.С., Черемушкін А.В. Основи криптографії: Навчальний посібникМ .: Геліос АРВ, 2001.

2. . Морозенко В.В., Генетический алгоритм для криптоанализа шифра Винжера, Вестник пермского университета, Пермь, 210.

3. Шнайер Б. Прикладна криптографія. протоколи, алгоритми, вихідні тексти на мові Сі.- М .: видавництво ТРІУМФ, 2002.

.