გენეტიკური ალგორითმების გამოყენება კრიპტოანალიზში

ზურაბ ქოჩლაძე*, ლალი ბესელია**
*ივ. ჯავახიშვილის სახელობის თბილისის სახელმწიფო უნივერსიტეტი,
ი. ვეკუას სახელობის გამოყენებითი მათემატიკის ინსტიტუტი, თბილისი, საქართველო,
zurab.kochladze62@gmail.com
**სოხუმის სახელმწიფო უნივერსიტეტი, თბილისი, საქართველო, lali.tibua@mail.ru

ამ ნაშრომში განხილულია გენეტიკური ალგორითმების გამოყენება კრიპტოანალიზში. გენეტიკური ალგორითმებს თავდაპირველად იყენებდნენ ოპტიმზაციის ამოცანების ამოსახსნელად. დროთა განმავლობაში მან გამოყენება ჰპოვა მეცნიერების სხვადასხვა დარგებში. ჩვენი მიზანია, ვაჩვენოთ გენეტიკური ალგორითმების გამოყენების უპირატესობა კრიპტოანალიზში სხვა მეთოდებთან შედარებით. სწორედ ამ თვალსაზრისით ავიღეთ მერკლი-ჰელმანის კრიპტოსისტემა [1,2], რომლის გატეხვასაც შევეცადეთ გენეტიკური ალგორით-მების გამოყენებით და ჩვენ მიერ მიღებული შედეგები შევადარეთ შამირის ალგორითმის მიერ მიღებულ შედეგებთან [3]. არსებობს რამდენიმე შრომა, სადაც მერკლი–ჰელმანის კრიპტოსისტემას ხსნიან გენეტიკური ალგორითმების საშუალებით, მაგრამ ყველა ამ შემთხვევაში შეტევა ხდება შიფროტექსტის საფუძველზე [4,5]. ამ შრომებისაგან განსხვავებით, მსგავსად შამირის მეთოდისა ჩვენ ვეძებთ საიდუმლო გასაღებს ღია გასაღებზე შეტევით. შევიმუშავეთ ახალი ევრისტიკული მეთოდები, რომლის შედეგადაც გენეტიკური ალგორითმების გამოყენება გავხადეთ უფრო ზუსტი და სწრაფი. ამ ნაშრომში მოცემული კვლევის შედეგები და პროგრამული უზრუნველყოფა გვაძლევს საშუალებას გამოვიტანოთ დასკვნა, რომ ჩვენს მიერ აგებული ალგორითმი შეიძლება გამოვიყენოთ სხვა ასიმეტრიული კრიპტოსისტემების კრიპტოანალიზისთვისაც.

ლიტერატურა

1. Merkle R.C., Hellman M.E.: Hidding information and signatures in trapdoor Knapsak, IEEE Trans. Inform. Theory, IT-24 (1978), pp. 535-530
2. Martello S., Toth P.: Knapsack problems John Wiley and Sons 1990.
3. Salomaa A.: Public-key Cryptography Springer-Verlag 1990
4. Garg P., Shastri A.: An Improved Cryptanalytic Attack on Knapsack Cipher using Genetic Algorithm. International Journal of Information Technology 3:3 2007.
5. Muthuregunathan R., Vekataraman D., Rajasekaran P.: Cryptanalysis of Knapsack Ciher Using Parrallel Evolutionary Computing. International Journal of Recent Trends in Engineering, Vol. 1, No 1, May 2009.