Tweakable ბლოკური ალგორითმი ჰილის მოდიფიცირებული ალგორითმის გამოყენებით

ზურაბ ქოჩლაძე

Zurab.kochladze@tsu.ge

კომპიუტერულ მეცნიერებათა დეპარტამენტი,

აუსტ საბუნებისმეტყველო მეცნიერებათა ფაკულტეტი.

ივ. ჯავახიშვილის თბილისის სახელმწიფო უნივერსიტეტი

ი. ჭავჭავაძის გამზ. 1

საკვანძო სიტყვები: *tweakable ბლოკური შიფრი, ჰილის მოდიფიცირებული ალგორითმი.*

ცნობილ ჰილის ალგორითმში ღია ტექსტი გადადის რიცხვით ვექტორიში და შემდეგ მრავლდება შებრუნებად მატრიცაზე. ამ ალგორითმის ძირითად უპირატესობას სხვა ალგორითმებთან შედარებით წარმოადგენს ის, რომ დაშიფრული ტექსტის ერთი სიმბოლოს გამომუშავებაში მონაწილეობს ღია ტექსტის რამდენიმე სიმბოლო, რაც ართულებს შიფრის კრიპტოანალიზს. ავტორის მიერ სტატიაში [1] შემოთავაზებული იყო ამ ალგორითმის მოდიფიკაცია, ნაცვლად ვექტორად გარდაქმნის, ღია ტექსტი გარდაიქმნება კვადრატულ მატრიცად, და შემდეგ ხდება მისი გამრავლება შებრუნებად მატრიცაზე. აქვე ნაჩვენები იყო, რომ ალგორითმი ინარჩუნებს თავის ძირითად თვისებას.

მოხსენებაში აღწერილია ამ მეთოდის გამოყენება tweakable ბლოკური ალგორითმის ასაგებად. ალგორითმი მუშაობს 128 ბიტის სიგრძის ბლოკებთან და იყენებს 256 ბიტიან გასაღებს. რაუნდში შესვლამდე ხდება საწყისი გასაღების პირველი (უფროსი) 128 ბიტის და ღია ტექსტი შეკრება ოპერაცია XOR-ის გამოყენებით. ამ ოპერაციის შემდეგ მიღებული 128 ბიტი შედის პირველ რაუნდში დასამუშავებლად. პირველი რაუნდული ოპერაციაა მიღებული ტექსტის XOR-ით შეკრება tweak პარამეტრთან. tweak პარამეტრი გამოყენება მხოლოდ კენტ რაუნდებში. ამ შეკრების შედეგად მიღებული 128 ბიტიანი ტექსტი გარდაიქმნება მატრიცად 4×4 და ხდება მისი გამრავლება თვითშებრუნებად მატრიცაზე. მიღებული მატრიცა კვლავ გარდაიქმნება 128 ბიტიან სტრიქონად და შეიკრიბება რაუნდულ გასაღებთან. ამის შემდეგ ხდება ამ მატრიცის შესვლა S ბლოკში. S ბლოკის სქემა აღებულია ცნობილი AES სტანდარტიდან, რომელიც ისეა აგებული, რომ გაუძლოს დიფერენციალურ და წრფივ შეტევებს. რაუნდული გასაღებების და tweake პარამეტრების გამომუშავება ხდება ასევე ჰილის მოდიფიცირებული ალგორითმის გამოყენებით. საწყისი გასაღები ჩაიწერება მატრიცის სახით და გამრავლდება თვითშებრუნებად მატრიცაზე. ეს წარმოადგენს პირველი რაუნდის გასაღებს. შემდეგი რაუნდების გასაღების გამოთვლაში მონაწილეობს წინა რაუნდის გასაღები. პარამეტრების მიღების პროცედურა ანალოგიურია რაუნდული გასაღებების მიღების პროცედურის. ალგორითმში ჰილის მოდიფიცირებული ალგორითმის გამოყენება საშუალებას იძლევა შევამციროთ რაუნდების რაოდენობა, რაც მნიშვნელოვნად ამცირებს დაშიფვრის დროს.

1. Z. Kochladze Modified Version of the Hill's Algorithm. GESJ: Computer Science and Telecommunication No3 (43) 2014.